

Pdf by:
<https://www.pro-memoria.info>

The Strengthened Code of Practice on Disinformation 2022

**The Strengthened
Code of Practice on
Disinformation
2022**

TABLE OF CONTENT

Pdf by:
<https://www.pro-memoria.info>

<u>I. PREAMBLE</u>	1
<u>II. SCRUTINY OF AD PLACEMENTS</u>	4
DEMONETISATION OF DISINFORMATION	5
TACKLING ADVERTISING CONTAINING DISINFORMATION	7
COOPERATION WITH RELEVANT PLAYERS	8
<u>III. POLITICAL ADVERTISING</u>	9
A COMMON UNDERSTANDING OF POLITICAL AND ISSUE ADVERTISING.....	10
EFFICIENT LABELLING OF POLITICAL OR ISSUE ADS	10
VERIFICATION COMMITMENTS FOR POLITICAL OR ISSUE ADS	11
USER-FACING TRANSPARENCY COMMITMENTS FOR POLITICAL OR ISSUE ADS	12
POLITICAL OR ISSUE AD REPOSITORIES AND MINIMUM FUNCTIONALITIES FOR APPLICATION PROGRAMMING INTERFACES (APIS) TO ACCESS POLITICAL OR ISSUE AD DATA.....	13
CIVIL SOCIETY COMMITMENTS	14
ONGOING COLLABORATION.....	14
<u>IV. INTEGRITY OF SERVICES</u>	15
COMMON UNDERSTANDING OF IMPERMISSIBLE MANIPULATIVE BEHAVIOUR.....	15
TRANSPARENCY OBLIGATIONS FOR AI SYSTEMS	17
COOPERATION AND TRANSPARENCY.....	17
<u>V. EMPOWERING USERS</u>	18
ENHANCING MEDIA LITERACY.....	19
‘SAFE DESIGN’ OF THE ARCHITECTURE OF THE SERVICES, TRANSPARENT POLICIES, AND ACCOUNTABILITY OF RECOMMENDER SYSTEMS.....	20
BETTER EQUIPPING USERS TO IDENTIFY DISINFORMATION.....	21
FUNCTIONALITY TO FLAG HARMFUL FALSE AND/OR MISLEADING INFORMATION.....	25
TRANSPARENT APPEAL MECHANISM.....	25
MEASURES TO CURB DISINFORMATION ON MESSAGING APPS.....	25
<u>VI. EMPOWERING THE RESEARCH COMMUNITY</u>	26
DISCLOSURE OF AND ACCESS TO SIGNATORIES’ DATA FOR RESEARCH ON DISINFORMATION ...	27
Automated access to non-personal data and anonymised, aggregated or manifestly made public data	27
Governance structure for access to data for research purposes requiring additional scrutiny	28
COOPERATION WITH RESEARCHERS	29
TRANSPARENCY AND DATA SHARING FROM RESEARCH ORGANISATIONS.....	30

<u>VII. EMPOWERING THE FACT-CHECKING COMMUNITY</u>	31
COOPERATION WITH THE FACT-CHECKING COMMUNITY	31
USE AND INTEGRATION OF FACT-CHECKING IN SIGNATORIES' SERVICES	33
FACT-CHECKERS' ACCESS TO RELEVANT INFORMATION	34
FACT-CHECKERS' STANDARDS.....	34
<u>VIII. TRANSPARENCY CENTRE</u>	35
<u>IX. PERMANENT TASK-FORCE</u>	36
<u>X. MONITORING OF THE CODE</u>	39

I. PREAMBLE

- (a) Following the European Commission Guidance on Strengthening the Code of Practice on Disinformation¹ (hereafter the “Guidance”), the European Commission’s Communication on the European Democracy Action Plan² (hereafter “EDAP”), the European Commission’s Communication “Tackling online disinformation: a European approach”³ (hereafter the “Communication”), the Council Conclusions of 28 June 2018⁴, and the various important initiatives taking place across Europe to address the challenges posed by the dissemination of disinformation⁵, the Signatories⁶ of the present Code of Practice (the “Code”) recognise their role in contributing to the fight against Disinformation, which for the rest of the Code is considered to include misinformation⁷, disinformation⁸, information influence operations⁹ and foreign interference¹⁰ in the information space¹¹ (Disinformation)
- (b) The Signatories recognise and agree with the European Commission’s conclusions that “[t]he exposure of citizens to large scale Disinformation, including misleading or outright false information, is a major challenge for Europe,” and that “[o]ur open democratic societies depend on public debates that allow well-informed citizens to express their will through free and fair political processes”.¹²
- (c) As stressed in the Communication, fundamental rights must be fully respected in all the actions taken to fight Disinformation¹³. The Signatories are mindful of the fundamental right to freedom of expression, freedom of information, and privacy, and of the delicate balance that must be struck between protecting fundamental rights and taking effective action to limit the spread and impact of otherwise lawful content.
- (d) The Signatories recognise that the dissemination of Disinformation has many facets, both online and offline, and is facilitated by and impacts a broad range of actors, and that all stakeholders in the ecosystem have roles to play in countering its spread.

¹ COM(2021)262final <https://digital-strategy.ec.europa.eu/en/library/guidance-strengthening-code-practice-disinformation>

² COM(2020)790 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423>

³ COM(2018)236 final http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51804

⁴ <http://www.consilium.europa.eu/media/35936/28-euco-final-conclusions-en.pdf>

⁵ Notwithstanding, the notion of “Disinformation” does not include misleading advertising, reporting errors, satire and parody, or clearly identified partisan news and commentary, and is without prejudice to binding legal obligations, self-regulatory advertising codes, and standards regarding misleading advertising.

⁶ Companies, organisations and associations listed on Annex [1]

⁷ As defined in EDAP: “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.

⁸ As defined in EDAP: “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”.

⁹ 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’.

¹⁰ 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’

¹¹ Disinformation may be addressed by multiple operational policies and tools that vary between signatories but nonetheless aim to address the challenges described.

¹² Communication, paragraph 1.

¹³ See the Communication, paragraph 3.1.1, where the European Commission states that all actions taken to challenge Disinformation “should strictly respect freedom of expression and include safeguards that prevent their misuse, for example, the censoring of critical, satirical, dissenting, or shocking speech. They should also strictly respect the European Commission’s commitment to an open, safe and reliable Internet”.

- (e) The Signatories note the important achievements of the 2018 Code of Practice¹⁴ and are building on these, while recognising the need to further strengthen the Code in order to be a more efficient instrument in fighting Disinformation, as set out in the Guidance.

It is in this spirit that the Signatories have drafted the present Code identifying the commitment areas and measures each Signatory is making.

- (f) Signatories agree to sign up to Commitments and Measures that are of relevance to the product(s), activities, and service(s) they and their subsidiaries offer and identify in the subscription document the relevant Commitments and Measures they will implement and will also specify the relevant services covered by such Commitments and Measures. If a signatory does not sign up to a commitment or measure because it is not relevant or pertinent for their services, it will explain the reasons for this in the subscription document (where relevant at service level).
- (g) The Signatories agree to regularly review their Commitments and Measures, to consider subscribing to additional Commitments and Measures as they become relevant, pertinent, and practicable, taking into account inputs on these matters from the Code's Task-force. The Signatories are also able to bring to the rest of the Task-force's attention Commitments or Measures that may benefit from changes over time as their practices and approaches evolve and in view of technological, societal, market and legislative developments.
- (h) Actions under the Code will complement and be aligned with regulatory requirements and overall objectives in the Digital Services Act (DSA)¹⁵ once it enters into force. The DSA will set out a co-regulatory framework, including through voluntary Codes of Conduct or other co-regulatory measures, aimed at addressing systemic risks by the Very Large Online Platforms¹⁶, including those linked to Disinformation.
- (i) This Code of Practice aims to become a Code of Conduct under Article 35 of the DSA, after entry into force, regarding Very Large Online Platforms that sign up to its Commitments and Measures.
- (j) As indicated in the Guidance, Very Large Online Platforms need to take robust measures to identify (risk assessment) and address (risk mitigation) the relevant systemic risks under the proposed DSA. Therefore, signing up to all Commitments relevant and pertinent to their services should be considered as a possible risk mitigation measure under article 27 of the DSA.
- (k) To facilitate the participation in the Code of Signatories that provide services that do not qualify as Very Large Online Platforms, it is recognised that they are encouraged to subscribe to Commitments that are relevant to their services and to implement them through measures that are proportionate in light of the size and nature of their services and the resources available to them.
- (l) To this end, signatories that are not Very Large Online Platforms have the option to identify in the subscription document measures proportionate and appropriate to their services that they will implement to fulfil the Commitments subscribed to, and/or a plan to achieve over time full implementation of the measures set out in the Code for the Commitments concerned. In such cases, Signatories concerned shall identify the Qualitative Reporting Elements (QRE) and Service Level Indicators (SLI) they will provide regarding these Measures. The Task-force shall regularly

¹⁴ SWD(2020)180 <https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement>

¹⁵ As defined in the Section 4 of the 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 European Commission.

¹⁶ As defined in the Article [25] of [DSA], the provisions of the Code addressed to the Very Large Online Platforms should cover as well all the entities to which the obligations of the Section 4 of the final text of the DSA will apply.

review the consistency of such adapted measures with the effective functioning of the Code. In view of ensuring that reporting requirements are proportionate, the Task-force will develop a simplified reporting template for these signatories. In their reporting, these Signatories shall confirm on an annual basis whether the continued adapted application of the Commitments and Measures concerned is still relevant and pertinent.

- (m) Signatories who help address the spread of Disinformation through their tools, technical efforts, philanthropic work, or specific expertise, commit to sign up to Commitments and Measures that are attuned to the company or organisation and the role they play in the online ecosystem.
- (n) The Signatories recognise that trade associations which have signed this Code are not entering into obligations due to their nature on behalf of their members. However, these associations commit to make their members fully aware of this Code, and encourage them to join it or respect its principles, as appropriate.
- (o) The Signatories will implement the Commitments and the Measures to which they have signed up within six months after signature of the Code. Within seven months of signature, the Signatories will provide the European Commission with baseline reports detailing how they have implemented their Commitments under the Code and provide the Qualitative Reporting Elements (QREs) and Service Level Indicators (SLIs), as they stand one month after the implementation - recognising that the baseline report will be the very first report provided by the Signatories' and as such may require improvements, and that Signatories' reports may become more detailed over time. The first reporting should also include a comparison between the measures in place under the previous Code to the measures taken to implement the new Code.
- (p) The Signatories recognise the need to cooperate with the European Commission in assessing the reporting on the functioning of the Code, including by making appropriate information available upon reasonable request and by responding to the European Commission's questions and consultations. The Signatories also recognise the need to closely cooperate with and involve the European Regulators Group for Audiovisual Media Services (ERGA) and the European Digital Media Observatory (EDMO), in particular in the implementation phase and in the monitoring phase of the Code.
- (q) The Code shall apply within the framework of existing laws of the EU and its Member States and must not be construed in any way as replacing, superseding or interpreting the existing and future legal framework, and, in particular (but not limited to):
 - The EU Charter of Fundamental Rights;
 - The European Convention on Human Rights;
 - Directive 2000/31/EC, with particular reference to Articles 12 to 15, which shall apply to any obligation of this Code targeting or assumed by mere conduits, caching providers, or hosting providers such as providers of network, search engines, browsers, online blogging platforms, online forums, video-sharing platforms, social media, etc.;
 - Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;
 - Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector;
 - Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market;
 - Directive 2006/114/EC concerning misleading and comparative advertising;
 - Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services;

- Directive 2018/1808 concerning the provision of audiovisual media services;
 - Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure;
 - Regulation 2019/1150 on promoting fairness and transparency for business users of online intermediation services;
 - The case law of the CJEU and ECHR on the proportionality of measures designed to limit access to and circulation of harmful content.
- (r) This Code is without prejudice to other initiatives aimed at tackling Disinformation.
- (s) This Code is agreed in good faith between the Signatories, building on a fair and honest representation of their intentions.
- (t) The application of this Code is limited for each Signatory to services provided in the States that are Contracting Parties to the European Economic Area.
- (u) A Signatory may withdraw from the Code by notifying the Task-force. Such a withdrawal will not have the effect of terminating the Code between the other Signatories.
- (v) Additional signatories may sign the Code at any time. To this end, candidate signatories must present their activities to the Task-force, along with the Commitments and Measures that they intend to sign up under the Code, in line with the principles set out in this Preamble.

II. SCRUTINY OF AD PLACEMENTS

Whereas:

- (a) The Signatories recognise the priorities outlined in 2021 European Commission's Guidance¹⁷ and bearing in mind that the commercial aspect is only one of the many facets of Disinformation, the Signatories acknowledge the need to "significantly improve the scrutiny of advertisement placements, notably in order to reduce revenues of the purveyors of Disinformation"¹⁸.
- (b) The Signatories recognise their collective and individual accountabilities to work together to defund Disinformation in advertising and media across the following types of organisations and their respective responsibilities; advertisers and agencies who are involved in the purchasing of advertising space; publishers¹⁹ and platforms who are involved in the selling of advertising space and approval of advertising campaigns; advertising technology companies who are involved in the targeting or selection of advertising space and/or content and verification reporting; auditing bodies who are involved the accreditation of services ranging from targeting to reporting. All of these parties commit their individual resources and collaborate to ensure that the advertising industry bars the placement of harmful Disinformation campaigns and the selling of advertising space from Disinformation pages.

¹⁷ European Commission Guidance on Strengthening the Code of Practice on Disinformation, COM(2021) 262 final, 26 May 2021, Section 6.1, page 12.

¹⁸ Tackling online disinformation: a European Approach, COM(2018) 36 final, 26 April 2018.

¹⁹ A publisher is an operator of a website, app or other content where digital advertisements are displayed or user information is collected and used for digital advertising, such as Website owners, blog owners, podcast productions, video content creators, mobile apps/games, etc.

- (c) The Signatories recognise the need to strengthen and expand existing commitments aimed at defunding the dissemination of Disinformation²⁰ on Signatories' own services or on third-party websites.
- (d) The Signatories recognise the need to combat the dissemination of harmful Disinformation via advertising messages and services.
- (e) Relevant Signatories recognise the need to take granular and tailored action to address Disinformation risks linked to the distribution of online advertising. Actions will be applicable to all online advertising.
- (f) Relevant Signatories recognise the importance of implementing policies and processes not to accept remuneration from Disinformation actors, or otherwise promote such accounts and websites.
- (g) The Signatories recognise that all parties involved in the buying and selling of online advertising and the provision of advertising-related services need to work together to improve transparency across the online advertising ecosystem and thereby to effectively scrutinise, control and limit the placement of advertising on accounts and websites belonging to purveyors of Disinformation.
- (h) Avoiding the misplacement of advertising on online Disinformation websites requires further refinement of already widely used brand safety tools to successfully continue to meet this challenge, in recognition of the nature of this content.²¹ The Signatories recognise the need to improve the availability and uptake of brand safety tools.
- (i) The Signatories recognise that the integration of information from and cooperation with third-party organisations providing information and solutions regarding Disinformation content are important to reduce monetisation of Disinformation.

Therefore, the Signatories of this Code commit to the following:

DEMONETISATION OF DISINFORMATION

Commitment 1. Relevant Signatories participating in ad placements, commit to defund the dissemination of Disinformation, and improve the policies and systems which determine the eligibility of content to be monetised, the controls for monetisation and ad placement, and the data to report on the accuracy and effectiveness of controls and services around ad placements.

In order to satisfy Commitment 1:

Measure 1.1. Relevant Signatories involved in the selling of advertising, inclusive of media platforms, publishers and ad tech companies, will deploy, disclose, and enforce policies with the aims of:

- first avoiding the publishing and carriage of harmful Disinformation to protect the integrity of advertising supported businesses
- second taking meaningful enforcement and remediation steps to avoid the placement of advertising next to Disinformation content or on sources that repeatedly violate these policies; and
- third adopting measures to enable the verification of the landing / destination pages of ads and origin of ad placement.

²⁰ "The notion of "Disinformation" does not include misleading advertising, reporting errors, satire and parody, or clearly identified partisan news and commentary, and is without prejudice to binding legal obligations, self-regulatory advertising codes, and standards regarding misleading advertising."

²¹ Communication 'Tackling online Disinformation: a European Approach', http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51804.

Relevant Signatories will set up a working group and work on developing a methodology to report on demonetisation efforts, including data related to the volume of advertising that support Disinformation sources, while taking account of legal constraints related to financial reporting and methodological challenges, and present a recommendation to the Task-force within 6 months, to include an additional SLI for the baseline reports. The SLI should provide insight into the impact of actions taken by relevant Signatories at the service and the Member State levels.

ORE 1.1.1: Signatories will disclose and outline the policies they develop, deploy, and enforce to meet the goals of Measure 1.1 and will link to relevant public pages in their help centres.

SLI 1.1.1: Signatories will report, quantitatively, on actions they took to enforce each of the policies mentioned in the qualitative part of this service level indicator, at the Member State or language level. This could include, for instance, actions to remove, to block, or to otherwise restrict advertising on pages and/or domains that disseminate harmful Disinformation.

Measure 1.2. Relevant Signatories responsible for the selling of advertising, inclusive of publishers, media platforms, and ad tech companies, will tighten eligibility requirements and content review processes for content monetisation and ad revenue share programmes on their services as necessary to effectively scrutinise parties and bar participation by actors who systematically post content or engage in behaviours which violate policies mentioned in Measure 1.1 that tackle Disinformation.

ORE 1.2.1: Signatories will outline their processes for reviewing, assessing, and augmenting their monetisation policies in order to scrutinise and bar participation by actors that systematically provide harmful Disinformation.

SLI 1.2.1: Signatories will report on the number of policy reviews and/or updates to policies relevant to Measure 1.2 throughout the reporting period. In addition, Signatories will report on the numbers of accounts or domains barred from participation to advertising or monetisation as a result of these policies at the Member State level, if not already covered by metrics shared under Measure 1.1 above.

Measure 1.3. Relevant Signatories responsible for the selling of advertising, inclusive of publishers, media platforms, and ad tech companies, will take commercial and technically feasible steps, including support for relevant third-party approaches, to give advertising buyers transparency on the placement of their advertising.

ORE 1.3.1: Signatories will report on the controls and transparency they provide to advertising buyers with regards to the placement of their ads as it relates to Measure 1.3.

Measure 1.4. Relevant Signatories responsible for the buying of advertising, inclusive of advertisers, and agencies, will place advertising through ad sellers that have taken effective, and transparent steps to avoid the placement of advertising next to Disinformation content or in places that repeatedly publish Disinformation.

ORE 1.4.1: Relevant Signatories that are responsible for the buying of advertising will describe their processes and procedures to ensure they place advertising through ad sellers that take the steps described in Measure 1.4.

Measure 1.5. Relevant Signatories involved in the reporting of monetisation activities inclusive of media platforms, ad networks, and ad verification companies will take the necessary steps to give industry-recognised relevant independent third-party auditors commercially appropriate and fair access to their services and data in order to:

- First, confirm the accuracy of first party reporting relative to monetisation and Disinformation, seeking alignment with regular audits performed under the DSA.
- Second, accreditation services should assess the effectiveness of media platforms' policy enforcement, including Disinformation policies.

ORE 1.5.1: Signatories that produce first party reporting will report on the access provided to independent third-party auditors as outlined in Measure 1.5 and will link to public reports and

results from such auditors, such as MRC Content Level Brand Safety Accreditation, TAG Brand Safety certifications, or other similarly recognised industry accepted certifications.

ORE 1.5.2: Signatories that conduct independent accreditation via audits will disclose areas of their accreditation that have been updated to reflect needs in Measure 1.5.

Measure 1.6. Relevant Signatories will advance the development, improve the availability, and take practical steps to advance the use of brand safety tools and partnerships, with the following goals:

- To the degree commercially viable, relevant Signatories will provide options to integrate information and analysis from source-raters, services that provide indicators of trustworthiness, fact-checkers, researchers or other relevant stakeholders providing information e.g., on the sources of Disinformation campaigns to help inform decisions on ad placement by ad buyers, namely advertisers and their agencies.
- Advertisers, agencies, ad tech companies, and media platforms and publishers will take effective and reasonable steps to integrate the use of brand safety tools throughout the media planning, buying and reporting process, to avoid the placement of their advertising next to Disinformation content and/or in places or sources that repeatedly publish Disinformation.
- Brand safety tool providers and rating services who categorise content and domains will provide reasonable transparency about the processes they use, insofar that they do not release commercially sensitive information or divulge trade secrets, and that they establish a mechanism for customer feedback and appeal.

ORE 1.6.1: Signatories that place ads will report on the options they provide for integration of information, indicators and analysis from source raters, services that provide indicators of trustworthiness, fact-checkers, researchers, or other relevant stakeholders providing information e.g. on the sources of Disinformation campaigns to help inform decisions on ad placement by buyers.

ORE 1.6.2: Signatories that purchase ads will outline the steps they have taken to integrate the use of brand safety tools in their advertising and media operations, disclosing what percentage of their media investment is protected by such services (both qualitative reporting element + SLI).

ORE 1.6.3: Signatories that provide brand safety tools will outline how they are ensuring transparency and appealability about their processes and outcomes.

ORE 1.6.4: Relevant Signatories that rate sources to determine if they persistently publish Disinformation shall provide reasonable information on the criteria under which websites are rated, make public the assessment of the relevant criteria relating to Disinformation, operate in an apolitical manner and give publishers the right to reply before ratings are published.

SLI 1.6.1: Signatories that purchase ads will outline the steps they have taken to integrate the use of brand safety tools in their advertising and media operations, disclosing what percentage of their media investment is protected by such services.

TACKLING ADVERTISING CONTAINING DISINFORMATION

Commitment 2. Relevant Signatories participating in advertising commit to prevent the misuse of advertising systems to disseminate Disinformation in the form of advertising messages.

In order to satisfy Commitment 2:

Measure 2.1. Relevant Signatories will develop, deploy, and enforce appropriate and tailored advertising policies that address the misuse of their advertising systems for propagating harmful Disinformation in advertising messages and in the promotion of content.

ORE 2.1.1: Signatories will disclose and outline the policies they develop, deploy, and enforce to meet the goals of Measure 2.1 and will link to relevant public pages in their help centres.

SLI 2.1.1: Signatories will report, quantitatively, on actions they took to enforce each of the policies mentioned in the qualitative part of this service level indicator, at the Member State or language level. This could include, for instance, actions to remove, to block, or to otherwise restrict harmful Disinformation in advertising messages and in the promotion of content.

Measure 2.2. Relevant Signatories will develop tools, methods, or partnerships, which may include reference to independent information sources both public and proprietary (for instance partnerships with fact-checking or source rating organisations, or services providing indicators of trustworthiness, or proprietary methods developed internally) to identify content and sources as distributing harmful Disinformation, to identify and take action on ads and promoted content that violate advertising policies regarding Disinformation mentioned in Measure 2.1.

ORE 2.2.1: Signatories will describe the tools, methods, or partnerships they use to identify content and sources that contravene policies mentioned in Measure 2.1 - while being mindful of not disclosing information that'd make it easier for malicious actors to circumvent these tools, methods, or partnerships. Signatories will specify the independent information sources involved in these tools, methods, or partnerships.

Measure 2.3. Relevant Signatories will adapt their current ad verification and review systems as appropriate and commercially feasible, with the aim of preventing ads placed through or on their services that do not comply with their advertising policies in respect of Disinformation to be inclusive of advertising message, promoted content, and site landing page.

ORE 2.3.1: Signatories will describe the systems and procedures they use to ensure that ads placed through their services comply with their advertising policies as described in Measure 2.1.

SLI 2.3.1: Signatories will report quantitatively, at the Member State level, on the ads removed or prohibited from their services using procedures outlined in Measure 2.3. In the event of ads successfully removed, parties should report on the reach of violatory content and advertising.

Measure 2.4. Relevant Signatories will provide relevant information to advertisers about which advertising policies have been violated when they reject or remove ads violating policies described in Measure 2.1 above or disable advertising accounts in application of these policies and clarify their procedures for appeal.

ORE 2.4.1: Signatories will describe how they provide information to advertisers about advertising policies they have violated and how advertisers can appeal these policies.

SLI 2.4.1: Signatories will report quantitatively, at the Member State level, on the number of appeals per their standard procedures they received from advertisers on the application of their policies and on the proportion of these appeals that led to a change of the initial policy decision.

COOPERATION WITH RELEVANT PLAYERS

Commitment 3. Relevant Signatories involved in buying, selling and placing digital advertising commit to exchange best practices and strengthen cooperation with relevant players, expanding to organisations active in the online monetisation value chain, such as online e-payment services, e-commerce platforms and relevant crowd-funding/donation systems, with the aim to increase the effectiveness of scrutiny of ad placements on their own services.

In order to satisfy Commitment 3:

Measure 3.1. Relevant Signatories will cooperate with platforms, advertising supply chain players, source-rating services, services that provide indicators of trustworthiness, fact-checking organisations, advertisers and any other actors active in the online monetisation value chain, to facilitate the integration and flow of information, in particular information relevant for tackling purveyors of harmful Disinformation, in full respect of all relevant data protection rules and confidentiality agreements.

ORE 3.1.1: Signatories will outline how they work with others across industry and civil society to facilitate the flow of information that may be relevant for tackling purveyors of harmful Disinformation.

Measure 3.2. Relevant Signatories will exchange among themselves information on Disinformation trends and TTPs (Tactics, Techniques, and Procedures), via the Code Task-force, GARM, IAB Europe, or other relevant fora. This will include sharing insights on new techniques or threats observed by Relevant Signatories, discussing case studies, and other means of improving capabilities and steps to help remove Disinformation across the advertising supply chain - potentially including real-time technical capabilities.

ORE 3.2.1: Signatories will report on their discussions within fora mentioned in Measure 3.2, being mindful of not disclosing information that is confidential and/or that may be used by malicious actors to circumvent the defences set by Signatories and others across the advertising supply chain. This could include, for instance, information about the fora Signatories engaged in; about the kinds of information they shared; and about the learnings they derived from these exchanges.

Measure 3.3. Relevant Signatories will integrate the work of or collaborate with relevant third-party organisations, such as independent source-rating services, services that provide indicators of trustworthiness, fact-checkers, researchers, or open-source investigators, in order to reduce monetisation of Disinformation and avoid the dissemination of advertising containing Disinformation.

ORE 3.3.1: Signatories will report on the collaborations and integrations relevant to their work with organisations mentioned.

III. POLITICAL ADVERTISING

Whereas:

- (a) The Signatories recognise the importance of political and issue advertising in shaping political campaigns and public debates around key societal issues, particularly in forming public opinion, political and electoral debate, referenda, legislative processes and the voting behaviour of citizens.
- (b) The Signatories acknowledge that any advertiser (including media organisations and companies) can run political or issue ads.
- (c) The Signatories acknowledge the importance of collaborating together towards the development of a shared understanding of “political advertising”, seeking alignment with the European Commission’s proposal for a Regulation on the transparency and targeting of political advertising, and of their approach to compliance with the relevant provisions of that proposed regulation and the DSA, in particular with respect to the definitions and obligations established in those regulations.
- (d) The Signatories also acknowledge the need to collaborate on a shared understanding of “issue advertising” taking into account the European Commission’s proposal for a Regulation on the transparency and targeting of political advertising and the DSA.
- (e) The Signatories also acknowledge the significance of a shared understanding of “sponsor” in the context of the European Commission’s proposal for a Regulation on the transparency and targeting of political advertising.
- (f) The Signatories recognise the importance of ensuring political ads are run neutrally regardless of the political orientation or the issue addressed.

- (g) Through the present strengthened Code, the Signatories agree to contribute to transparency of political advertising and to ensure additional protection of personal data when it is used in the context of targeting political advertising, in full compliance with the GDPR and other relevant laws, in particular with regard to acquiring valid consent where required.

Therefore, the Signatories of this Code commit to the following:

A COMMON UNDERSTANDING OF POLITICAL AND ISSUE ADVERTISING

Commitment 4. Relevant Signatories commit to adopt a common definition of “political and issue advertising”.

In order to satisfy Commitment 4:

Measure 4.1. Relevant Signatories commit to define "political and issue advertising" in this section in line with the definition of "political advertising" set out in the European Commission's proposal for a Regulation on the transparency and targeting of political advertising.

Measure 4.2. Should there be no political agreement on the definition of “political advertising” in the context of the negotiations on the European Commission's proposal for a Regulation on the transparency and targeting of political advertising within the first year of the Code's operation or should this Regulation not include a definition of “political advertising” which adequately covers “issue advertising” (as assessed in the Task-force under QRE 4.1.1), the Signatories will come together with the Task-force to establish working definitions of political advertising and issue advertising that can serve as baseline for this chapter.

ORE 4.1.1: (for Measures 4.1 and 4.2) Relevant Signatories will declare the relevant scope of their commitment at the time of reporting and publish their relevant policies, demonstrating alignment with the European Commission's proposal for a Regulation on the transparency and targeting of political advertising.

ORE 4.1.2: (for Measures 4.1 and 4.2) After the first year of the Code's operation, Relevant Signatories will state whether they assess that further work with the Task-force is necessary and the mechanism for doing so, in line with Measure 4.2.

Commitment 5. Relevant Signatories commit to apply a consistent approach across political and issue advertising on their services and to clearly indicate in their advertising policies the extent to which such advertising is permitted or prohibited on their services.

In order to satisfy Commitment 5:

Measure 5.1. Relevant Signatories will apply the labelling, transparency and verification principles (as set out below) across all ads relevant to their Commitments 4 and 5. They will publicise their policy rules or guidelines pertaining to their service's definition(s) of political and/or issue advertising in a publicly available and easily understandable way.

ORE 5.1.1: Relevant Signatories will report on their policy rules or guidelines and on their approach towards publicising them.

EFFICIENT LABELLING OF POLITICAL OR ISSUE ADS

Commitment 6. Relevant Signatories commit to make political or issue ads clearly labelled and distinguishable as paid-for content in a way that allows users to understand that the content displayed contains political or issue advertising.

In order to satisfy Commitment 6:

Measure 6.1. Relevant Signatories will develop a set of common best practices and examples for marks and labels on political or issue ads and integrate those learnings as relevant to their services.

ORE 6.1.1: Relevant Signatories will publicise the best practises and examples developed as part of Measure 2.2.1 and describe how they relate to their relevant services.

Measure 6.2. Relevant Signatories will ensure that relevant information, such as the identity of the sponsor, is included in the label attached to the ad or is otherwise easily accessible to the user from the label.

ORE 6.2.1: Relevant Signatories will publish examples of how sponsor identities and other relevant information are attached to ads or otherwise made easily accessible to users from the label.

ORE 6.2.2: Relevant Signatories will publish their labelling designs.

SLI 6.2.1: Relevant Signatories will publish meaningful metrics, at Member State level, on the volume of ads labelled according to Measure 6.2, such as the number of ads accepted and labelled, amounts spent by labelled advertisers, or other metrics to be determined in discussion within the Task-force with the aim to assess the efficiency of this labelling.

Measure 6.3. Relevant Signatories will invest and participate in research to improve users' identification and comprehension of labels, discuss the findings of said research with the Task-force, and will endeavour to integrate the results of such research into their services where relevant.

ORE 6.3.1: Relevant Signatories will publish relevant research into understanding how users identify and comprehend labels on political or issue ads and report on the steps they have taken to ensure that users are consistently able to do so and to improve the labels' potential to attract users' awareness.

Measure 6.4. Relevant Signatories will ensure that once a political or issue ad is labelled as such on their platform, the label remains in place when users share that same ad on the same platform, so that they continue to be clearly identified as paid-for political or issue content.

ORE 6.4.1: Relevant Signatories will describe the steps they put in place to ensure that labels remain in place when users share ads.

Measure 6.5. Relevant Signatories that provide messaging services will, where possible and when in compliance with local law, use reasonable efforts to work towards improving the visibility of labels applied to political advertising shared over messaging services. To this end they will use reasonable efforts to develop solutions that facilitate users recognising, to the extent possible, paid-for content labelled as such on their online platform when shared over their messaging services, without any weakening of encryption and with due regard to the protection of privacy.

ORE 6.5.1. Relevant Signatories will report on any solutions in place to empower users to recognise paid-for content as outlined in Measure 6.5.

VERIFICATION COMMITMENTS FOR POLITICAL OR ISSUE ADS

Commitment 7. Relevant Signatories commit to put proportionate and appropriate identity verification systems in place for sponsors and providers of advertising services acting on behalf of sponsors placing political or issue ads. Relevant signatories will make sure that labelling and user-facing transparency requirements are met before allowing placement of such ads.

In order to satisfy Commitment 7:

Measure 7.1. Relevant Signatories will make sure the sponsors and providers of advertising services acting on behalf of sponsors purchasing political or issue ads have provided the relevant information regarding their identity to verify (and re-verify where appropriate) said identity or the sponsors they are acting on behalf of before allowing placement of such ads.

ORE 7.1.1: Relevant Signatories will report on the tools and processes in place to collect and verify the information outlined in Measure 7.1.1, including information on the timeliness and proportionality of said tools and processes.

SLI 7.1.1: Relevant Signatories will publish meaningful metrics on the volume of ads rejected for failure to fulfil the relevant verification processes, comparable to metrics for SLI 6.2.1, where relevant per service and at Member State level.

Measure 7.2. Relevant Signatories will complete verifications processes described in Commitment 7 in a timely and proportionate manner.

ORE 7.2.1: Relevant Signatories will report on the actions taken against actors demonstrably evading the said tools and processes, including any relevant policy updates.

ORE 7.2.2: Relevant Signatories will provide information on the timeliness and proportionality of the verification process.

Measure 7.3. Relevant Signatories will take appropriate action, such as suspensions or other account-level penalties, against political or issue ad sponsors who demonstrably evade verification and transparency requirements via on-platform tactics. Relevant Signatories will develop - or provide via existing tools - functionalities that allow users to flag ads that are not labelled as political.

ORE 7.3.1: Relevant Signatories will report on the tools and processes in place to request a declaration on whether the advertising service requested constitutes political or issue advertising.

ORE 7.3.2: Relevant Signatories will report on policies in place against political or issue ad sponsors who demonstrably evade verification and transparency requirements on-platform.

Measure 7.4. Relevant Signatories commit to request that sponsors, and providers of advertising services acting on behalf of sponsors, declare whether the advertising service they request constitutes political or issue advertising.²²

ORE 7.4.1: Relevant Signatories will report on research and publish data on the effectiveness of measures they take to verify the identity of political or issue ad sponsors.

USER-FACING TRANSPARENCY COMMITMENTS FOR POLITICAL OR ISSUE ADS

Commitment 8. Relevant Signatories commit to provide transparency information to users about the political or issue ads they see on their service.

In order to satisfy Commitment 8:

Measure 8.1. Relevant Signatories will agree on the common minimum transparency obligations, seeking alignment with the European Commission's proposal for a Regulation on the transparency and targeting of political advertising, such as identification of the sponsor, display period, ad spend, and aggregate information on recipients of the ad.

²² Where relevant, the methods deemed acceptable for verification and identification of political advertisements and advertisers under the Regulation on the transparency and targeting of political advertising will be considered acceptable for Signatories' commitments under this Code.

Measure 8.2. Relevant Signatories will provide a direct link from the ad to the ad repository.

ORE 8.1.1 (for Measures 8.1 and 8.2): Relevant Signatories will publicise the common minimum transparency obligations developed as part of Measures 8.1 and 8.2 and describe how they relate to their relevant services, including the data available to the user.

Commitment 9. Relevant Signatories commit to provide users with clear, comprehensible, comprehensive information about why they are seeing a political or issue ad.

In order to satisfy Commitment 9:

Measure 9.1. Relevant Signatories will, seeking alignment with the European Commission's proposal for a Regulation on the transparency and targeting of political advertising, provide a simple means for users to access information about why they are seeing a particular political or issue ad.

Measure 9.2. Relevant Signatories will explain in simple, plain language, the rationale and the tools used by the sponsors and providers of advertising services acting on behalf of sponsors (for instance: demographic, geographic, contextual, interest or behaviourally-based) to determine that a political or issue ad is displayed specifically to the user.

ORE 9.1.1 (for Measures 9.1 and 9.2): Relevant Signatories will describe the tools and features in place to provide users with the information outlined in Measures 9.1 and 9.2, including relevant examples for each targeting method offered by the service.

POLITICAL OR ISSUE AD REPOSITORIES AND MINIMUM FUNCTIONALITIES FOR APPLICATION PROGRAMMING INTERFACES (APIs) TO ACCESS POLITICAL OR ISSUE AD DATA.

Commitment 10. Relevant Signatories commit to maintain repositories of political or issue advertising and ensure their currentness, completeness, usability and quality, such that they contain all political and issue advertising served, along with the necessary information to comply with their legal obligations and with transparency commitments under this Code.

In order to satisfy Commitment 10:

Measure 10.1. Relevant Signatories will set up and maintain dedicated searchable ad repositories containing accurate records (in as close to real time as possible, in particular during election periods) of all political and issue ads served, including the ads themselves. This should be accompanied by relevant information for each ad such as the identification of the sponsor; the dates the ad ran for; the total amount spent on the ad; the number of impressions delivered; the audience criteria used to determine recipients; the demographics and number of recipients who saw the ad; and the geographical areas the ad was seen in.

Measure 10.2. The information in such ad repositories will be publicly available for at least 5 years.²³

ORE 10.2.1 (for Measures 10.1 and 10.2): Relevant Signatories will detail the availability, features, and updating cadence of their repositories to comply with Measures 10.1 and 10.2. Relevant Signatories will also provide quantitative information on the usage of the repositories, such as monthly usage.

Commitment 11. Relevant Signatories commit to provide application programming interfaces (APIs) or other interfaces enabling users and researchers to perform customised searches within their ad repositories of political or issue advertising and to include a set of minimum functionalities as well as a set of minimum search criteria for the application of APIs or other interfaces.

²³ Signatories will align the minimum time for availability in ads repositories as it may emerge under the framework of the European Commission's proposal for a Regulation on the transparency and targeting of political advertising.

In order to satisfy Commitment 11:

- Measure 11.1. Relevant Signatories' APIs or other interfaces will provide 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 (in particular during elections) in standard formats, including for instance searches per advertiser or candidate, per geographic area or country, per language, per keyword, per election, or per other targeting criteria, to allow for research and monitoring.
- Measure 11.2. The data Relevant Signatories make available via such APIs and other interfaces will be equivalent to or more detailed than that data made available through their ad repositories.
- Measure 11.3. Relevant Signatories will ensure wide access to and availability of APIs and other interfaces.
- Measure 11.4. Relevant Signatories will engage with researchers and update the functionalities of the APIs and other interfaces to meet researchers' reasonable needs where applicable.

ORE 11.1.1 (for Measures 11.1-11.4): Relevant Signatories will detail the availability and features of APIs or other interfaces to comply with Measures 11.1 – 11.4. Relevant Signatories will also provide quantitative information on the usage of the APIs, such as monthly usage.

ORE 11.4.1: Relevant Signatories will report about their engagement with researchers, including to understand their experience with the functionalities of APIs, and the resulting improvements of the functionalities as the result of this engagement and of a discussion within the Task-force.

CIVIL SOCIETY COMMITMENTS

Commitment 12. Relevant Signatories commit to increase oversight of political and issue advertising and constructively assist, as appropriate, in the creation, implementation and improvement of political or issue advertising policies and practices.

In order to satisfy Commitment 12:

- Measure 12.1. Relevant Signatories will work to research, monitor and report on the use of online political or issue advertising across Member States.
- Measure 12.2. Relevant Signatories will produce tools, dashboards and other data to ensure proper scrutiny of political or issue advertising, particularly during election periods in Member States.
- Measure 12.3. Relevant Signatories will alert fellow Signatories to issues in the implementation or enforcement of political or issue advertising policies or of this Code.

ORE 12.1.1 (for Measures 12.1-12.3): Relevant Signatories will share their research and findings publicly and with the Task-force for discussion and potential follow-up actions.

ONGOING COLLABORATION

Commitment 13. Relevant Signatories agree to engage in ongoing monitoring and research to understand and respond to risks related to Disinformation in political or issue advertising.

In order to satisfy Commitment 13:

- Measure 13.1. Relevant Signatories agree to work individually and together through the Task-force to identify novel and evolving disinformation risks in the uses of political or issue advertising and discuss options for addressing those risks.
- Measure 13.2. Relevant Signatories will consult with the Task-force and other relevant stakeholders to assess the opportunity and impact of short election "blackout periods" for political or issue advertising on their services in all Member States.
- Measure 13.3. Relevant Signatories agree to evaluate, together with the Task-force, whether there is sufficient independent scrutiny of political or issue advertising in Member States.

ORE 13.1.1 (for Measures 13.1-13.3): Through the Task-force, the Relevant Signatories will convene, at least annually, an appropriately resourced discussion around:

- novel risks in political advertising to develop coordinated policy
- ongoing discussions on blackout periods
- independent scrutiny of political or issue advertising.

IV. INTEGRITY OF SERVICES

Whereas:

- (a) Relevant Signatories recognise the importance of intensifying and demonstrating the effectiveness of efforts to ensure the integrity of services by implementing and promoting safeguards against both misinformation and disinformation, including impermissible manipulative behaviours and practices across their services, as defined in the Preamble.
- (b) For this purpose and in order to facilitate reporting and dialogue under the Code, in line with the 2021 European Commission’s Guidance, Relevant Signatories acknowledge the importance of collaborating together towards the development of a common understanding on impermissible manipulative behaviours and practices across their services, without prejudice to existing EU and national laws compatible with Article 10 of the European Convention on Human Rights and Articles 11, 47 and 52 of the Charter of Fundamental Rights of the Union.
- (c) In addition, the Relevant Signatories recognise the necessity to continue to strengthen their commitments in order to counter and limit impermissible manipulative behaviours and practices across their services, foreign information manipulation and interference, and hybrid threats to security.
- (d) Relevant Signatories aim to collaborate together in drawing up a comprehensive list of shared terminology of impermissible manipulative behaviours and practices, which should periodically be amended in light with the latest evidence on the conducts and tactics, techniques and procedures (TTPs) employed by malicious actors, in particular to the AMITT Disinformation Tactics, Techniques and Procedures Framework. Such collaboration could take place in the framework of the permanent Task-force set by this Code.
- (e) In order to ensure continued relevance and adequacy, the Relevant Signatories agree to intensify their efforts in terms of transparency to their users as well as accountability on impermissible manipulative and inauthentic behaviours and practices across their services.
- (f) Consistent with Article 8 of the European Convention on Human Rights and Article 7 and 8 of the European Charter of Fundamental Rights, Relevant Signatories reiterate the importance not to prohibit anonymous or pseudonymous use of accounts and services.

Therefore, the Relevant Signatories of this Code commit to the following:

COMMON UNDERSTANDING OF IMPERMISSIBLE MANIPULATIVE BEHAVIOUR

Commitment 14. In order to limit impermissible manipulative behaviours and practices across their services, Relevant Signatories commit to put in place or further bolster policies to address both misinformation and disinformation across their services, and to agree on a cross-service understanding of manipulative behaviours, actors and practices not permitted on their services.

Such behaviours and practices, which should periodically be reviewed in light with the latest evidence on the conducts and TTPs employed by malicious actors, such as the AMITT Disinformation Tactics, Techniques and Procedures Framework, include:

- **The creation and use of fake accounts, account takeovers and bot-driven amplification,**
- **Hack-and-leak operations,**
- **Impersonation,**
- **Malicious deep fakes,**
- **The purchase of fake engagements,**
- **Non-transparent paid messages or promotion by influencers,**
- **The creation and use of accounts that participate in coordinated inauthentic behaviour,**
- **User conduct aimed at artificially amplifying the reach or perceived public support for disinformation.**

In order to satisfy Commitment 14:

Measure 14.1. Relevant Signatories will adopt, reinforce and implement clear policies regarding impermissible manipulative behaviours and practices on their services, based on the latest evidence on the conducts and tactics, techniques and procedures (TTPs) employed by malicious actors, such as the AMITT Disinformation Tactics, Techniques and Procedures Framework.

ORE 14.1.1: Relevant Signatories will list relevant policies and clarify how they relate to the threats mentioned above as well as to other Disinformation threats.

ORE 14.1.2: Signatories will report on their proactive efforts to detect impermissible content, behaviours, TTPs and practices relevant to this commitment.

Measure 14.2. Relevant Signatories will keep a detailed, up-to-date list of their publicly available policies that clarifies behaviours and practices that are prohibited on their services and will outline in their reports how their respective policies and their implementation address the above set of TTPs, threats and harms as well as other relevant threats. Such information will also be reported in the Transparency Centre. The list of TTPs will serve as the base for the TTPs to be reported upon and relevant signatories will work within the Permanent Task-force to further develop and refine related indicators on the impact/effectiveness of their related actions. Relevant Signatories will also develop further metrics to estimate the penetration and impact that Fake/Inauthentic accounts have on genuine users and report at the Member State level (including trends on audiences targeted; narratives used etc.).

ORE 14.2.1: Relevant Signatories will report on actions taken to implement the policies they list in their reports and covering the range of TTPs identified/employed, at the Member State level.

SLI 14.2.1: Number of instances of identified TTPs and actions taken at the Member State level under policies addressing each of the TTPs as well as information on the type of content.

SLI 14.2.2: Views/impressions of and interaction/engagement at the Member State level (e.g. likes, shares, comments), related to each identified TTP, before and after action was taken.

SLI 14.2.3: [once available] Metrics to estimate the penetration and impact that e.g. Fake/Inauthentic accounts have on genuine users and report at the Member State level (including trends on audiences targeted; narratives used etc.).

SLI 14.2.4: Estimation, at the Member State level, of TTPs related content, views/impressions and interaction/engagement with such content as a percentage of the total content, views/impressions and interaction/engagement on relevant signatories' service [for TTPs where such prevalence estimate is possible to compute].

Measure 14.3. Relevant Signatories will convene via the Permanent Task-force to agree upon and publish a list and terminology of TTPs employed by malicious actors, which should be updated on an

annual basis, and consist in a shared understanding of manipulative behaviours and practices not permitted on their service to-date. On that basis, they will aim to develop common baseline elements, objectives, and benchmarks for the policies and measures deployed to counter such manipulative behaviours and practices.

ORE 14.3.1: Signatories will report on the list of TTPs agreed in the Permanent Task-force within 6 months of the signing of the Code and will update this list at least every year. They will also report about the common baseline elements, objectives and benchmarks for the policies and measures. They will also update the Transparency Centre with this information.

TRANSPARENCY OBLIGATIONS FOR AI SYSTEMS

Commitment 15. Relevant Signatories that develop or operate AI systems and that disseminate AI-generated and manipulated content through their services (e.g. deepfakes) commit to take into consideration the transparency obligations and the list of manipulative practices prohibited under the proposal for Artificial Intelligence Act.

In order to satisfy Commitment 15:

Measure 15.1. Relevant signatories will establish or confirm their policies in place for countering prohibited manipulative practices for AI systems that generate or manipulate content, such as warning users and proactively detect such content.

ORE 15.1.1: In line with EU and national legislation, Relevant Signatories will report on their policies in place for countering prohibited manipulative practices for AI systems that generate or manipulate content.

Measure 15.2. Relevant Signatories will establish or confirm their policies in place to ensure that the algorithms used for detection, moderation and sanctioning of impermissible conduct and content on their services are trustworthy, respect the rights of end-users and do not constitute prohibited manipulative practices impermissibly distorting their behaviour in line with Union and Member States legislation.

ORE 15.2.1: Relevant Signatories will report on their policies and actions to ensure that the algorithms used for detection, moderation and sanctioning of impermissible conduct and content on their services are trustworthy, respect the rights of end-users and do not constitute prohibited manipulative practices in line with Union and Member States legislation.

COOPERATION AND TRANSPARENCY

Commitment 16. Relevant Signatories commit to operate channels of exchange between their relevant teams in order to proactively share information about cross-platform influence operations, foreign interference in information space and relevant incidents that emerge on their respective services, with the aim of preventing dissemination and resurgence on other services, in full compliance with privacy legislation and with due consideration for security and human rights risks.

In order to satisfy Commitment 16:

Measure 16.1. Relevant Signatories will share relevant information about cross-platform information manipulation, foreign interference in information space and incidents that emerge on their respective services for instance via a dedicated sub-group of the permanent Task-force or via existing fora for exchanging such information.

ORE 16.1.1: Relevant Signatories will disclose the fora they use for information sharing as well as information about learnings derived from this sharing.

SLI 16.1.1: Number of actions taken as a result of the collaboration and information sharing between signatories. Where they have such information, they will specify which Member States that were affected (including information about the content being detected and acted upon due to this collaboration).

Measure 16.2. Relevant Signatories will pay specific attention to and share information on the tactical migration of known actors of misinformation, disinformation and information manipulation across different platforms as a way to circumvent moderation policies, engage different audiences or coordinate action on platforms with less scrutiny and policy bandwidth.

ORE 16.2.1: As a result of the collaboration and information sharing between them, Relevant Signatories will share qualitative examples and case studies of migration tactics employed and advertised by such actors on their platforms as observed by their moderation team and/or external partners from Academia or fact-checking organisations engaged in such monitoring.

V. EMPOWERING USERS

Whereas:

- (a) The Signatories recognise the importance of empowering users to detect and report false and/or misleading content as a key tool to limit the impact of disinformation. In this context, signatories recognise the importance of diluting the visibility and permeation of Disinformation by continuing to improve the findability of trustworthy content, enhance the safe design of their services and empower users with dedicated tools to identify disinformation and empowering users with tools to detect and report these types of content, as referred in the 2021 European Commission's Guidance²⁴.
- (b) The Signatories recognise the importance of the potential of provenance technology to empower users with tools to interrogate the provenance and authenticity of content to help the users determining the veracity of content.
- (c) The Signatories recognise the importance of enhancing their efforts in the area of media literacy including to protect and empower vulnerable groups.
- (d) The Signatories also recognise the importance of intensifying their actions for a safer design and architecture of their services in order to mitigate the risks of viral propagation of D.
- (e) The Signatories acknowledge the significant impact that recommender systems have on the information diet of users, and therefore recognise that recommender systems should be transparent and provide users with the possibility to modify at any time their preferred options for the way that information is recommended to them.
- (f) The Signatories recognise that facilitating user access to tools that can support their assessment of the factual accuracy of sources for example through fact-checks from independent fact-checking organisations or warning labels from other authoritative sources, is crucial to curbing the disinformation phenomena.
- (g) For this purpose, the Signatories consider it important to research on the feasibility and effectiveness of developing warnings or updates targeted to users that have interacted with content that was later removed for violation of their policies.
- (h) The Signatories that provide private messaging applications recognise the importance to test and implement technical features helping users to identify and flag disinformation disseminated

²⁴ European Commission Guidance on Strengthening the Code of Practice on Disinformation, COM(2021) 262 final, 26 May 2021, Section 6.1, page 12.

through such services and explore with fact-checkers privacy-compliant opportunities to integrate their work into such services.

- (i) Consistently with Article 10 of the European Convention on Human Rights and Articles 7, 8, 11, 47 and 52 of the Charter of Fundamental Rights of the Union, actions taken by signatories on harmful false and/or misleading content flagged by users should respect the freedom of expression, the right to private communications, the protection of personal data, and user's right to an effective remedy and shall not be disproportionate.

Therefore, the Relevant Signatories of this Code commit to the following:

ENHANCING MEDIA LITERACY

Commitment 17. In light of the European Commission's initiatives in the area of media literacy, including the new Digital Education Action Plan, Relevant Signatories commit to continue and strengthen their efforts in the area of media literacy and critical thinking, also with the aim to include vulnerable groups.

In order to satisfy Commitment 17:

Measure 17.1. Relevant Signatories will design and implement or continue to maintain tools to improve media literacy and critical thinking, for instance by empowering users with context on the content visible on services or with guidance on how to evaluate online content.

ORE 17.1.1: Relevant Signatories will outline the tools they develop or maintain that are relevant to this commitment and report on their deployment in each Member State.

SLI 17.1.1: Relevant Signatories will report, at the Member State level, on metrics pertinent to assessing the effects of the tools described in the qualitative reporting element for Measure 17.1, which will include: the total count of impressions of the tool; and information on the interactions/engagement with the tool.

Measure 17.2. Relevant Signatories will develop, promote and/or support or continue to run activities to improve media literacy and critical thinking such as campaigns to raise awareness about Disinformation, as well as the TTPs that are being used by malicious actors, among the general public across the European Union, also considering the involvement of vulnerable communities.

ORE 17.2.1: Relevant Signatories will describe the activities they launch or support and the Member States they target and reach. Relevant signatories will further report on actions taken to promote the campaigns to their user base per Member States targeted.

SLI 17.2.1: Relevant Signatories report on number of media literacy and awareness raising activities organised and or participated in and will share quantitative information pertinent to show the effects of the campaigns they build or support at the Member State level (for instance: list of Member States where those activities took place; reach of campaigns; engagement these activities have generated; number of interactions with online assets; number of participants).

Measure 17.3. For both of the above Measures, and in order to build on the expertise of media literacy experts in the design, implementation, and impact measurement of tools, relevant Signatories will partner or consult with media literacy experts in the EU, including for instance the Commission's Media Literacy Expert Group, ERGA's Media Literacy Action Group, EDMO, its country-specific branches, or relevant Member State universities or organisations that have relevant expertise.

ORE 17.3.1: Relevant Signatories will describe how they involved and partnered with media literacy experts for the purposes of all Measures in this Commitment.

‘SAFE DESIGN’ OF THE ARCHITECTURE OF THE SERVICES, TRANSPARENT POLICIES, AND ACCOUNTABILITY OF RECOMMENDER SYSTEMS

Commitment 18. Relevant Signatories commit to minimise the risks of viral propagation of Disinformation by adopting safe design practices as they develop their systems, policies, and features.

In order to satisfy Commitment 18:

Measure 18.1. Relevant Signatories will take measures to mitigate risks of their services fuelling the viral spread of harmful Disinformation, such as:

- recommender systems designed to improve the prominence of authoritative information and reduce the prominence of Disinformation based on clear and transparent methods and approaches for defining the criteria for authoritative information;
- other systemic approaches in the design of their products, policies, or processes, such as pre-testing.

ORE 18.1.1: Relevant Signatories will report on the risk mitigation systems, tools, procedures, or features deployed under Measure 18.1 and report on their deployment in each EU Member State.

ORE 18.1.2: Relevant Signatories will publish the main parameters of their recommender systems, both in their report and, once it is operational, on the Transparency Centre.

ORE 18.1.3: Relevant Signatories will outline how they design their products, policies, or processes, to reduce the impressions and engagement with Disinformation whether through recommender systems or through other systemic approaches, and/or to increase the visibility of authoritative information.

SLI 18.1.1: Relevant Signatories will provide, through meaningful metrics capable of catering for the performance of their products, policies, processes (including recommender systems), or other systemic approaches as relevant to Measure 18.1 an estimation of the effectiveness of such measures, such as the reduction of the prevalence, views, or impressions of Disinformation and/or the increase in visibility of authoritative information. Insofar as possible, Relevant Signatories will highlight the causal effects of those measures.

Measure 18.2. Relevant Signatories will develop and enforce publicly documented, proportionate policies to limit the spread of harmful false or misleading information (as depends on the service, such as prohibiting, downranking, or not recommending harmful false or misleading information, adapted to the severity of the impacts and with due regard to freedom of expression and information); and take action on webpages or actors that persistently violate these policies.

ORE 18.2.1: Relevant Signatories will report on the policies or terms of service that are relevant to Measure 18.2 and on their approach towards persistent violations of these policies.

SLI 18.2.1: Relevant Signatories will report on actions taken in response to violations of policies relevant to Measure 18.2, at the Member State level. The metrics shall include:

- Total number of violations
- Meaningful metrics to measure the impact of these actions (such as their impact on the visibility of or the engagement with content that was actioned upon)

Measure 18.3. Relevant Signatories will invest and/or participate in research efforts on the spread of harmful Disinformation online and related safe design practices, will make findings available to the public or report on those to the Code’s taskforce. They will disclose and discuss findings within the permanent Task-force, and explain how they intend to use these findings to improve existing safe design practices and features or develop new ones.

ORE 18.3.1: Relevant Signatories will describe research efforts, both in-house and in partnership with third-party organisations, on the spread of harmful Disinformation online and relevant safe design practices, as well as actions or changes as a result of this research. Relevant Signatories will include where possible information on financial investments in said research. Wherever possible, they will make their findings available to the general public.

Commitment 19. Relevant Signatories using recommender systems commit to make them transparent to the recipients regarding the main criteria and parameters used for prioritising or deprioritising information, and provide options to users about recommender systems, and make available information on those options.

In order to satisfy Commitment 19:

Measure 19.1. Relevant Signatories will make available to their users, including through the Transparency Centre and in their terms and conditions, in a clear, accessible and easily comprehensible manner, information outlining the main parameters their recommender systems employ.

ORE 19.1.1: Relevant Signatories will provide details of the policies and measures put in place to implement the above-mentioned measures accessible to EU users, especially by publishing information outlining the main parameters their recommender systems employ in this regard. This information should also be included in the Transparency Centre.

Measure 19.2. Relevant Signatories will provide options for the recipients of the service to select and to modify at any time their preferred options for relevant recommender systems, including giving users transparency about those options.

SLI 19.2.1: Relevant Signatories will provide aggregated information on effective user settings, such as the number of times users have actively engaged with these settings within the reporting period or over a sample representative timeframe, and clearly denote shifts in configuration patterns.

Commitment 20. Relevant Signatories commit to empower users with tools to assess the provenance and edit history or authenticity or accuracy of digital content.

In order to satisfy Commitment 20:

Measure 20.1. Relevant Signatories will develop technology solutions to help users check authenticity or identify the provenance or source of digital content, such as new tools or protocols or new open technical standards for content provenance (for instance, C2PA).

ORE 20.1.1: Relevant Signatories will provide details of the progress made developing provenance tools or standards, milestones reached in the implementation and any barriers to progress.

Measure 20.2. Relevant Signatories will take steps to join/support global initiatives and standards bodies (for instance, C2PA) focused on the development of provenance tools.

ORE 20.2.1: Relevant Signatories will provide details of global initiatives and standards bodies focused on the development of provenance tools (for instance, C2PA) that signatories have joined, or the support given to relevant organisations, providing links to organisation websites where possible.

BETTER EQUIPPING USERS TO IDENTIFY DISINFORMATION

Commitment 21. Relevant Signatories commit to strengthen their efforts to better equip users to identify Disinformation. In particular, in order to enable users to navigate services in an informed way, Relevant Signatories commit to facilitate, across all Member States languages

in which their services are provided, user access to tools for assessing the factual accuracy of sources through fact-checks from fact-checking organisations that have flagged potential Disinformation, as well as warning labels from other authoritative sources.

In order to satisfy Commitment 21:

Measure 21.1. Relevant Signatories will further develop and apply policies, features, or programs across Member States and EU languages to help users benefit from the context and insights provided by independent fact-checkers or authoritative sources, for instance by means of labels, such as labels indicating fact-checker ratings, notices to users who try to share or previously shared the rated content, information panels, or by acting upon content notified by fact-checkers that violate their policies. When cooperating with independent fact-checkers to label content on their services, Relevant Signatories will further develop and apply tools or features to inform users, through measures such as labels and notices, that content they interact with has been rated by an independent fact-checker and work to implement them across all EU Member States languages.

ORE 21.1.1: Relevant Signatories will report on the policies, features, or programs they deploy to meet this Measure and on their availability across Member States. When cooperating with independent fact-checkers to label content on their services, Relevant Signatories will report on:

- Independent fact-checkers they work with to label content on their services (unless a fact-checking organisation opposes such disclosure on the basis of a reasonable fear of retribution or violence), the languages they operate in, the policies they work under, and any labelling applied
- any tools or features available to inform users that content they interact with has been rated by an independent fact-checker

SLI 21.1.1: Relevant Signatories will report through meaningful metrics on actions taken under Measure 21.1, at the Member State level. Depending on the policies, features or programs in question, this could include reporting on actions taken under relevant policies; on reach of labels or fact-checks and other authoritative sources; or other similarly relevant metrics. At the minimum, the metrics will include: total impressions of fact-checks; ratio of impressions of fact-checks to original impressions of the fact-checked content—or if these are not pertinent to the implementation of fact-checking on their services, other equally pertinent metrics and an explanation of why those are more adequate.

SLI 21.1.2: When cooperating with independent fact-checkers to label content on their services, Relevant Signatories will report on actions taken at the Member State level and their impact, via metrics, of:

- number of articles published by independent fact-checkers
- number of labels applied to content, such as on the basis of such articles
- meaningful metrics on the impact of actions taken under Measure 21.1.1 such as the impact of said measures on user interactions with, or user re-shares of, content fact-checked as false or misleading.

Measure 21.2. Relevant Signatories will, in light of scientific evidence and the specificities of their services, and of user privacy preferences, undertake and/or support research and testing on warnings or updates targeted to users that have interacted with content that was later actioned upon for violation of policies mentioned in this section. They will disclose and discuss findings within the permanent Task-force in view of identifying relevant follow up actions.

ORE 21.2.1: Relevant Signatories will report on the research or testing efforts that they supported and undertook as part of this commitment and on the findings of research or testing undertaken as

part of this commitment. Wherever possible, they will make their findings available to the general public.

Measure 21.3. Where Relevant Signatories employ labelling and warning systems, they will design these in accordance with up-to-date scientific evidence and with analysis of their users' needs on how to maximise the impact and usefulness of such interventions, for instance such that they are likely to be viewed and positively received.

ORE 21.3.1: Relevant Signatories will report on their procedures for developing and deploying labelling or warning systems and how they take scientific evidence and their users' needs into account to maximise usefulness.

Commitment 22. Relevant Signatories commit to provide users with tools to help them make more informed decisions when they encounter online information that may be false or misleading, and to facilitate user access to tools and information to assess the trustworthiness of information sources, such as indicators of trustworthiness for informed online navigation, particularly relating to societal issues or debates of general interest.

In order to satisfy Commitment 22:

Measure 22.1. Relevant Signatories will make it possible for users of their services to access indicators of trustworthiness (such as trust marks focused on the integrity of the source and the methodology behind such indicators) developed by independent third-parties, in collaboration with the news media, including associations of journalists and media freedom organisations, as well as fact-checkers and other relevant entities, that can support users in making informed choices.

ORE 22.1.1: Relevant Signatories will report on how they enable users of their services to benefit from such indicators or trust marks.

SLI 22.1.1: Relevant Signatories will report on Member State level percentage of users that have enabled the trustworthiness indicator.

Measure 22.2. Relevant Signatories will give users the option of having signals relating to the trustworthiness of media sources into the recommender systems or feed such signals into their recommender systems.

ORE 22.2.1: Relevant Signatories will report on whether and, if relevant, how they feed signals related to the trustworthiness of media sources into their recommender systems, and outline the rationale for their approach.

Measure 22.3. Relevant Signatories will make details of the policies and measures put in place to implement the above-mentioned measures accessible to EU users, especially by publishing information outlining the main parameters their recommender systems employ in this regard. This information should also be included in the Transparency Centre.

ORE 22.3.1: Relevant Signatories will provide details of the policies and measures put in place to implement the above-mentioned measures accessible to EU users, especially by publishing information outlining the main parameters their recommender systems employ in this regard. This information should also be included in the Transparency Centre.

Measure 22.4. Relevant Signatories providing trustworthiness indicators will ensure that information sources are being reviewed in a transparent, apolitical, unbiased, and independent manner, applying fully disclosed criteria equally to all sources and allowing independent audits by independent regulatory authorities or other competent bodies.

ORE 22.4.1: Relevant Signatories will provide details of the basic criteria they use to review information sources and disclose relevant safeguards put in place to ensure that their services are apolitical, unbiased, and independent. They will provide examples of how these are applied

equally to a representative range of different publishers. Each analysis will indicate who contributed to assessing the source, or which certification body assessed the source.

SLI 22.4.1: Relevant Signatories, who have access to this data, will report on numbers measuring the volume of traffic for trustworthy sources generated thanks to the trustworthiness indicators.

Measure 22.5. Relevant Signatories providing trustworthiness indicators will provide compliance and correction mechanisms and respect the right of publishers to be heard, including to engage in the assessment process before indicators are applied and to have their responses available to consumers after assessments are published.

QRE 22.5.1: Relevant Signatories will publish regular corrections on their ratings or indicators if updates or mistakes occur. Relevant Signatories will provide examples of exchanges with publishers, including evidence of this engagement as recorded in trustworthiness indicators, and will regularly update their analysis to reflect any changes in the publications' practices, including any improvement of their practices.

SLI 22.5.1: Relevant signatories will report on the total number of instances per Member State where, following a publisher exercising its right to be heard before a rating or updated rating is issued, a rating of untrustworthy changes to a rating of trustworthy.

SLI 22.5.2: Relevant Signatories will report regularly on the number of publishers who have improved their journalistic practices after being assessed on the disclosed criteria and whose conformity, respectively trustworthiness scores thereby improved.

Measure 22.6. Relevant Signatories providing trustworthiness indicators by means of voluntary, self-regulatory and certifiable European standards or European standardisation deliverables as defined by European law ('technical standards')²⁵, such as the CWA17493:2019, will

- Develop and revise them based on internationally accepted best-practices and ethical norms;
- Make them publicly available and accessible in a non-proprietary, neutral way;
- Govern their implementation in line with European Accreditation and EU Regulation (EC) No 765/2008.

QRE 22.6.1: Relevant Signatories will publish self-evaluation and certification results of conforming entities as well as related statistics and analysis on engagement and conformity assessment, including complaints management.

SLI 22.6.1: Relevant Signatories will publish related statistics and analysis on engagement and conformity assessment, including complaints management.

Measure 22.7. Relevant Signatories will design and apply products and features (e.g. information panels, banners, pop-ups, maps and prompts, trustworthiness indicators) that lead users to authoritative sources on topics of particular public and societal interest or in crisis situations

QRE 22.7.1: Relevant Signatories will outline the products and features they deploy across their services and will specify whether those are available across Member States.

SLI 22.7.1: Relevant Signatories will report on the reach and/or user interactions with the products or features, at the Member State level, via the metrics of impressions and interactions (clicks, click-through rates (as relevant to the tools and services in question) and shares (as relevant to the tools and services in question)).

²⁵ Such as the Journalism Trust Initiative CWA17493:2019

FUNCTIONALITY TO FLAG HARMFUL FALSE AND/OR MISLEADING INFORMATION

Commitment 23. Relevant Signatories commit to provide users with the functionality to flag harmful false and/or misleading information that violates Signatories policies or terms of service.

In order to satisfy Commitment 23:

Measure 23.1. Relevant Signatories will develop or continue to make available on all their services and in all Member States languages in which their services are provided a user-friendly functionality for users to flag harmful false and/or misleading information that violates Signatories' policies or terms of service. The functionality should lead to appropriate, proportionate and consistent follow-up actions, in full respect of the freedom of expression.

ORE 23.1.1: Relevant Signatories will report on the availability of flagging systems for their policies related to harmful false and/or misleading information across EU Member States and specify the different steps that are required to trigger the systems.

Measure 23.2. Relevant Signatories will take the necessary measures to ensure that this functionality is duly protected from human or machine-based abuse (e.g., the tactic of 'mass-flagging' to silence other voices).

ORE 23.2.1: Relevant Signatories will report on the general measures they take to ensure the integrity of their reporting and appeals systems, while steering clear of disclosing information that would help would-be abusers find and exploit vulnerabilities in their defences.

TRANSPARENT APPEAL MECHANISM

Commitment 24. Relevant Signatories commit to inform users whose content or accounts has been subject to enforcement actions (content/accounts labelled, demoted or otherwise enforced on) taken on the basis of violation of policies relevant to this section (as outlined in Measure 18.2), and provide them with the possibility to appeal against the enforcement action at issue and to handle complaints in a timely, diligent, transparent, and objective manner and to reverse the action without undue delay where the complaint is deemed to be founded.

In order to satisfy Commitment 24:

Measure 24.1. Relevant Signatories commit to provide users with information on why particular content or accounts have been labelled, demoted, or otherwise enforced on, on the basis of violation of policies relevant to this section, as well as the basis for such enforcement action, and the possibility for them to appeal through a transparent mechanism.

ORE 24.1.1: Relevant Signatories will report on the availability of their notification and appeals systems across Member States and languages and provide details on the steps of the appeals procedure.

SLI 24.1.1: Relevant Signatories provide information on the number and nature of enforcement actions for policies described in response to Measure 18.2, the numbers of such actions that were subsequently appealed, the results of these appeals, information, and to the extent possible metrics, providing insight into the duration or effectiveness of processing of appeals process], and publish this information on the Transparency Centre.

MEASURES TO CURB DISINFORMATION ON MESSAGING APPS

Commitment 25. In order to help users of private messaging services to identify possible disinformation disseminated through such services, Relevant Signatories that provide messaging applications commit to continue to build and implement features or initiatives that empower users to think critically about information they receive and help them to determine

whether it is accurate, without any weakening of encryption and with due regard to the protection of privacy.

In order to satisfy Commitment 25:

Measure 25.1. Relevant Signatories will design and implement, or work with third-party partners to design and implement, features to facilitate users' access to authoritative information without any weakening of encryption and with due regard for the protection of privacy, third-party partners could include civil entities such as governments, fact-checkers, and other civil society organisations where appropriate. This could include (as is appropriate for each service), for example, digital literacy campaigns and programs, or third-party features to facilitate fact-checkers' or governments' use of the relevant messaging service to provide timely and accurate information to users.

ORE 25.1.1: Relevant Signatories will report on the tools, policies, partnerships, programs, and campaigns in place to meet this Measure and on their availability across Member States, including, where possible, relevant details on the civil entity and their results.

SLI 25.1.1: When in compliance with local law, and subject to any necessary information being made available by third-parties, Relevant Signatories will to the extent possible report on use of select tools (e.g. number of claims submitted by users to fact-checkers or reach of fact checks produced from claims submitted on the platform)

Measure 25.2. Relevant Signatories will develop tools and features that help users identify Disinformation and limit their viral propagation on their services, without any weakening of encryption and with due regard for the protection of privacy. This could include, for example, features to limit the forwarding of information across several conversations through additional friction or features making visible appropriate fact-checking labels when content from social media is disseminated over a messaging app (where possible).

ORE 25.2.1: Relevant Signatories will report on the tools and features available to limit the propagation of viral Disinformation on their services, and to empower users to think about the messages they receive.

SLI 25.2.1: When in compliance with local law and to the extent possible, without any weakening of encryption and with due regard to the protection of privacy, Relevant Signatories will provide a transparent estimation or evidence based research of the use and impact of tools, features, and campaigns deployed to meet Measures 25.1 and 25.2.

VI. EMPOWERING THE RESEARCH COMMUNITY

Whereas:

- (a) The Signatories acknowledge the importance of setting up a framework for robust access to platform data by the research community and adequate support for their activities as part of an effective strategy for tackling Disinformation.
- (b) A research proposal is qualified for the purposes of this Code if it is in line with relevant sector-related ethical and methodological best practices (as laid down, for example, in the EDMO proposal for a Code of Conduct on Access to Platform Data).
- (c) Signatories acknowledge that the research community can include civil society organisations whose primary goal is to conduct scientific research on a not-for-profit basis, pursuant to a public interest mission recognised by a Member State.
- (d) Consistently with Article 7 of the European Convention on Human Rights, Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), Signatories recognise that access conditions to

any data should respect the right to private communication and appropriately protect the rights and legitimate interests of all concerned parties.

- (e) Access to data for the purposes of this Code shall not be extended to government bodies and law enforcement authorities.
- (f) As a general principle, relevant Signatories recognise the importance of not prohibiting or discouraging good faith research into Disinformation on their platforms, and will not take adversarial action against the accounts of service users who undertake or participate in good-faith research into Disinformation.

Therefore, the Relevant Signatories of this Code commit to the following:

DISCLOSURE OF AND ACCESS TO SIGNATORIES' DATA FOR RESEARCH ON DISINFORMATION

Automated access to non-personal data and anonymised, aggregated or manifestly made public data²⁶

Commitment 26. Relevant Signatories commit to provide access, wherever safe and practicable, to continuous, real-time or near real-time, searchable stable access to non-personal data and anonymised, aggregated, or manifestly-made public data for research purposes on Disinformation through automated means such as APIs or other open and accessible technical solutions allowing the analysis of said data.

In order to satisfy Commitment 26:

Measure 26.1. Relevant Signatories will provide public access to non-personal data and anonymised, aggregated or manifestly-made public data pertinent to undertaking research on Disinformation on their services, such as engagement and impressions (views) of content hosted by their services, with reasonable safeguards to address risks of abuse (e.g. API policies prohibiting malicious or commercial uses).

ORE 26.1.1: Relevant Signatories will describe the tools and processes in place to provide public access to non-personal data and anonymised, aggregated and manifestly-made public data pertinent to undertaking research on Disinformation, as well as the safeguards in place to address risks of abuse.

ORE 26.1.2: Relevant Signatories will publish information related to data points available via Measure 25.1, as well as details regarding the technical protocols to be used to access these data points, in the relevant help centre. This information should also be reachable from the Transparency Centre. At minimum, this information will include definitions of the data points available, technical and methodological information about how they were created, and information about the representativeness of the data.

SLI 26.1.1: Relevant Signatories will provide quantitative information on the uptake of the tools and processes described in Measure 26.1, such as number of users.

Measure 26.2. Relevant Signatories will provide real-time or near real-time, machine-readable access to non-personal data and anonymised, aggregated or manifestly-made public data on their service for research purposes, such as accounts belonging to public figures such as elected official, news outlets and government accounts subject to an application process which is not overly cumbersome.

²⁶ The exact scope of “manifestly-made public data” will necessarily vary from service to service. Relevant Signatories will explain how this term applies to their service in their reporting.

ORE 26.2.1: Relevant Signatories will describe the tools and processes in place to provide real-time or near real-time access to non-personal data and anonymised, aggregated and manifestly-made public data for research purposes as described in Measure 26.2.

ORE 26.2.2: Relevant Signatories will describe the scope of manifestly-made public data as applicable to their services.

ORE 26.2.3: Relevant Signatories will describe the application process in place to in order to gain the access to non-personal data and anonymised, aggregated and manifestly-made public data described in Measure 26.2.

SLI 26.2.1: Relevant Signatories will provide meaningful metrics on the uptake, swiftness, and acceptance level of the tools and processes in Measure 26.2, such as:

- Number of monthly users (or users over a sample representative timeframe)
- Number of applications received, rejected, and accepted (over a reporting period or a sample representative timeframe)
- Average response time (over a reporting period or a sample representative timeframe).

Measure 26.3. Relevant Signatories will implement procedures for reporting the malfunctioning of access systems and for restoring access and repairing faulty functionalities in a reasonable time.

ORE 26.3.1: Relevant Signatories will describe the reporting procedures in place to comply with Measure 26.3 and provide information about their malfunction response procedure, as well as about malfunctions that would have prevented the use of the systems described above during the reporting period and how long it took to remediate them.

Governance structure for access to data for research purposes requiring additional scrutiny

Commitment 27. Relevant Signatories commit to provide vetted researchers with access to data necessary to undertake research on Disinformation by developing, funding, and cooperating with an independent, third-party body that can vet researchers and research proposals²⁷.

In order to satisfy Commitment 27:

Measure 27.1. Relevant Signatories commit to work with other relevant organisations (European Commission, Civil Society, DPAs) to develop within a reasonable timeline the independent third-party body referred to in Commitment 27, taking into account, where appropriate, ongoing efforts such as the EDMO proposal for a Code of Conduct on Access to Platform Data.

ORE 27.1.1: Relevant Signatories will describe their engagement with the process outlined in Measure 27.1 with a detailed timeline of the process, the practical outcome and any impacts of this process when it comes to their partnerships, programs, or other forms of engagement with researchers.

Measure 27.2. Relevant Signatories commit to co-fund from 2022 onwards the development of the independent third-party body referred to in Commitment 27.

ORE 27.2.1: Relevant Signatories will disclose their funding for the development of the independent third-party body referred to in Commitment 27.

Measure 27.3. Relevant Signatories commit to cooperate with the independent third-party body referred to in Commitment 27 once it is set up, in accordance with applicable laws, to enable sharing of personal data necessary to undertake research on Disinformation with vetted researchers in accordance with protocols to be defined by the independent third-party body.

²⁷ Signatories will align the procedures to vet researchers for the purpose of this section, as they may emerge under the framework of Article 31 DSA.

ORE 27.3.1: Relevant Signatories will describe how they cooperate with the independent third-party body to enable the sharing of data for purposes of research as outlined in Measure 27.3, once the independent third-party body is set up.

SLI 27.3.1: Relevant Signatories will disclose how many of the research projects vetted by the independent third-party body they have initiated cooperation with or have otherwise provided access to the data they requested.

Measure 27.4. Relevant Signatories commit to engage in pilot programs towards sharing data with vetted researchers for the purpose of investigating Disinformation, without waiting for the independent third-party body to be fully set up. Such pilot programmes will operate in accordance with all applicable laws regarding the sharing/use of data. Pilots could explore facilitating research on content that was removed from the services of Signatories and the data retention period for this content.

ORE 27.4.1: Relevant Signatories will describe the pilot programs they are engaged in to share data with vetted researchers for the purpose of investigating Disinformation. This will include information about the nature of the programs, number of research teams engaged, and where possible, about research topics or findings.

Commitment 28. COOPERATION WITH RESEARCHERS Relevant Signatories commit to support good faith research into Disinformation that involves their services.

In order to satisfy Commitment 28:

Measure 28.1. Relevant Signatories will ensure they have the appropriate human resources in place in order to facilitate research, and should set-up and maintain an open dialogue with researchers to keep track of the types of data that are likely to be in demand for research and to help researchers find relevant contact points in their organisations.

ORE 28.1.1: Relevant Signatories will describe the resources and processes they deploy to facilitate research and engage with the research community, including e.g. dedicated teams, tools, help centres, programs, or events.

Measure 28.2. Relevant Signatories will be transparent on the data types they currently make available to researchers across Europe.

ORE 28.2.1: Relevant Signatories will describe what data types European researchers can currently access via their APIs or via dedicated teams, tools, help centres, programs, or events.

Measure 28.3. Relevant Signatories will not prohibit or discourage genuinely and demonstratively public interest good faith research into Disinformation on their platforms, and will not take adversarial action against researcher users or accounts that undertake or participate in good-faith research into Disinformation.

ORE 28.3.1: Relevant Signatories will collaborate with EDMO to run an annual consultation of European researchers to assess whether they have experienced adversarial actions or are otherwise prohibited or discouraged to run such research.

Measure 28.4. As part of the cooperation framework between the Signatories and the European research community, relevant Signatories will, with the assistance of the EDMO, make funds available for research on Disinformation, for researchers to independently manage and to define scientific priorities and transparent allocation procedures based on scientific merit.

ORE 28.4.1: Relevant Signatories will disclose the resources made available for the purposes of Measure 28.4 and procedures put in place to ensure the resources are independently managed.

TRANSPARENCY AND DATA SHARING FROM RESEARCH ORGANISATIONS

Commitment 29. Relevant Signatories commit to conduct research based on transparent methodology and ethical standards, as well as to share datasets, research findings and methodologies with relevant audiences.²⁸

In order to satisfy Commitment 29:

Measure 29.1. Relevant Signatories will use transparent methodologies and ethical standards to conduct research activities that track and analyse influence operations, and the spread of Disinformation. They will share datasets, research findings and methodologies with members of the Task-force including EDMO, ERGA, and other Signatories and ultimately with the broader public.

QRE 29.1.1: Relevant Signatories will provide reports on their research, including topics, methodology, ethical standards, types of data accessed, data governance, and outcomes.

QRE 29.1.2: Relevant Signatories will update their research in the Transparency Centre to allow for greater awareness and availability of their work.

QRE 29.1.3: Relevant Signatories will provide detailed information on methodology development to all stakeholders informed about research results. They will also regularly inform all members of the Task-force, including ERGA, EDMO and other Signatories about research activities they conduct, and, wherever possible, the related methodologies used. They will finally share, wherever possible, such research outcomes and related methodologies with the broader public.

SLI 29.1.1: Relevant Signatories will report on the reach of stakeholders or citizens informed about the outcome of their research projects.

Measure 29.2. Relevant Signatories will conduct research activities that aim at ascertaining the relative effectiveness of various resilience-fostering measures implemented in the Code and elsewhere (e.g. labels, warnings, ex-post notifications), with a view to informing future regulatory and operational interventions.

QRE 29.2.1: Relevant Signatories will provide reports on their research, including topics, methodology, ethical standards, types of data accessed, data governance and outcomes.

QRE 29.2.2: Relevant Signatories will update their research in the Transparency Centre to allow for greater awareness and availability of their work.

QRE 29.2.3: Relevant Signatories will provide detailed information on methodology development to all stakeholders informed about research results. They will also regularly inform all members of the Task-force, including ERGA, EDMO and other Signatories about research activities they conduct, and, wherever possible, the related methodologies used. They will finally share, wherever possible, such research outcomes and related methodologies with the broader public.

SLI 29.2.1: Relevant Signatories will report on the reach of stakeholders or citizens informed about the outcome of their research projects.

Measure 29.3. Relevant Signatories will develop implementation models for effective repositories of advertising that aim at enhancing transparency with respect to advertising that contains Disinformation.

QRE 29.3.1: Relevant Signatories will update their research in the Transparency Centre to allow for greater awareness and availability regarding implementation models for effective repositories of advertising that aim at enhancing transparency of their work.

SLI 29.3.1: Relevant Signatories will report on the reach of stakeholders or citizens informed about the outcome of their research projects, research activities, methodologies and results.

²⁸ This is a reference to research output from research organisations signing on to this Commitment, rather than to data shared by platforms with said research organisations (under this Code or otherwise).

VII. EMPOWERING THE FACT-CHECKING COMMUNITY

Whereas:

- (a) The Signatories of this Code acknowledge the importance of setting up a framework for robust access to platform data by the fact-checking community and adequate support for their activities as part of an effective strategy for tackling Disinformation.
- (b) The Signatories recognise the importance of setting up 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, with a particular focus on Member States and languages where fact-checking is not yet provided.
- (c) To this aim, the Signatories underline the importance of consistently use and integrate fact-checkers' work in their platforms' services, including in programmatic advertising systems and in video content.
- (d) The Signatories underline the importance of providing fact-checkers with automated access to information on the actions they have taken with respect to fact-checked content and the fact checks, and also to other information that is pertinent to help them maximise the quality and impact of fact-checking.
- (e) The signatories recognise that for fact-checkers to be effective at fighting Disinformation, fact-checking organisations need to be verifiably independent from partisan institutions and transparent in their finances, organisation and methodology; as well as consistently and continuously dedicated to fact-checking either as verified signatories of the International Fact-checking Network Code of Principles (IFCN), members of the European Digital Media Observatory (EDMO)'s network of fact-checkers, or of the future Code of Professional Integrity for Independent European fact-checking organisations
- (f) Consistently with Article 7 of the European Convention on Human Rights, Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), the Signatories recognise that access conditions to any data should respect the right to private communications and appropriately protect the rights and legitimate interests of all concerned parties.

Therefore, the Relevant Signatories of this Code commit to the following:

COOPERATION WITH THE FACT-CHECKING COMMUNITY

Commitment 30. Relevant Signatories commit to establish a framework for transparent, structured, open, financially sustainable, and non-discriminatory cooperation between them and the EU fact-checking community regarding resources and support made available to fact-checkers.

In order to satisfy Commitment 30:

Measure 30.1. Relevant Signatories will set up agreements between them and independent fact-checking organisations (as defined in whereas (e)) to achieve fact-checking coverage in all Member States. These agreements should meet high ethical and professional standards and be based on

transparent, open, consistent and non-discriminatory conditions and will ensure the independence of fact-checkers.²⁹

ORE 30.1.1: Relevant Signatories will report on and explain the nature of their agreements with fact-checking organisations; their expected results; relevant quantitative information (for instance: contents fact-checked, increased coverage, changes in integration of fact-checking as depends on the agreements and to be further discussed within the Task-force); and such as relevant common standards and conditions for these agreements.

ORE 30.1.2: Relevant Signatories will list the fact-checking organisations they have agreements with (unless a fact-checking organisation opposes such disclosure on the basis of a reasonable fear of retribution or violence).

ORE 30.1.3: Relevant Signatories will report on resources allocated where relevant in each of their services to achieve fact-checking coverage in each Member State and to support fact-checking organisations' work to combat Disinformation online at the Member State level.

SLI 30.1.1: Relevant Signatories will report on Member States and languages covered by agreements with the fact-checking organisations, including the total number of agreements with fact-checking organisations, per language and, where relevant, per service.

Measure 30.2. Relevant Signatories will provide fair financial contributions to the independent European fact-checking organisations for their work to combat Disinformation on their services. Those financial contributions could be in the form of individual agreements, of agreements with multiple fact-checkers or with an elected body representative of the independent European fact-checking organisations that has the mandate to conclude said agreements.

ORE 30.2.1: Relevant Signatories will report on actions taken and general criteria used to ensure the fair financial contributions to the fact-checkers for the work done, on criteria used in those agreements to guarantee high ethical and professional standards, independence of the fact-checking organisations, as well as conditions of transparency, openness, consistency and non-discrimination.

ORE 30.2.2: Relevant Signatories will engage in, and report on, regular reviews with their fact-checking partner organisations to review the nature and effectiveness of the Signatory's fact-checking programme.

ORE 30.2.3: European fact-checking organisations will, directly (as Signatories to the Code) or indirectly (e.g. via polling by EDMO or an elected body representative of the independent European fact-checking organisations) report on the fairness of the individual compensations provided to them via these agreements.

Measure 30.3. Relevant Signatories will contribute to cross-border cooperation between fact-checkers.

ORE 30.3.1: Relevant Signatories will report on actions taken to facilitate their cross-border collaboration with and between fact-checkers, including examples of fact-checks, languages, or Member States where such cooperation was facilitated.

Measure 30.4. To develop the Measures above, relevant Signatories will consult EDMO and an elected body representative of the independent European fact-checking organisations.

ORE 30.4.1: Relevant Signatories will report, ex ante on plans to involve, and ex post on actions taken to involve, EDMO and the elected body representative of the independent European fact-checking organisations, including on the development of the framework of cooperation described in Measures 30.3 and 30.4.

²⁹ The Signatories commit to provide meaningful information under Commitment 29, while taking into account that certain information about individual agreements which may be commercially sensitive or confidential.

USE AND INTEGRATION OF FACT-CHECKING IN SIGNATORIES' SERVICES

Commitment 31. Relevant Signatories commit to integrate, showcase, or otherwise consistently use fact-checkers' work in their platforms' services, processes, and contents; with full coverage of all Member States and languages.

In order to satisfy Commitment 31:

Measure 31.1. Relevant Signatories that showcase User Generated Content (UGC) will integrate, showcase, or otherwise consistently use independent fact-checkers' work in their platforms' services, processes, and contents across all Member States and across formats relevant to the service. Relevant Signatories will collaborate with fact-checkers to that end, starting by conducting and documenting research and testing.

Measure 31.2. Relevant Signatories that integrate fact-checks in their products or processes will ensure they employ swift and efficient mechanisms such as labelling, information panels, or policy enforcement to help increase the impact of fact-checks on audiences.

ORE 31.1.1 (for Measures 30.1 and 30.2): Relevant Signatories will report on their specific activities and initiatives related to Measures 31.1 and 31.2, including the full results and methodology applied in testing solutions to that end.

SLI 31.1.1 (for Measures 30.1 and 30.2): Member State level reporting on use of fact-checks by service and the swift and efficient mechanisms in place to increase their impact, which may include (as depends on the service): number of fact-check articles published; reach of fact-check articles; number of content pieces reviewed by fact-checkers.

SLI 31.1.2 (for Measures 30.1 and 30.2): An estimation, through meaningful metrics, of the impact of actions taken such as, for instance, the number of pieces of content labelled on the basis of fact-check articles, or the impact of said measures on user interactions with information fact-checked as false or misleading.

SLI 31.1.3 (for Measures 30.1 and 30.2): Signatories recognise the importance of providing context to SLIs 31.1.1 and 31.1.2 in ways that empower researchers, fact-checkers, the Commission, ERGA, and the public to understand and assess the impact of the actions taken to comply with Commitment 31. To that end, relevant Signatories commit to include baseline quantitative information that will help contextualise these SLIs. Relevant Signatories will present and discuss within the Permanent Task-force the type of baseline quantitative information they consider using for contextualisation ahead of their baseline reports.

Measure 31.3. Relevant Signatories (including but not necessarily limited to fact-checkers and platforms) will create, in collaboration with EDMO and an elected body representative of the independent European fact-checking organisations, a repository of fact-checking content that will be governed by the representatives of fact-checkers. Relevant Signatories (i.e. platforms) commit to contribute to funding the establishment of the repository, together with other Signatories and/or other relevant interested entities. Funding will be reassessed on an annual basis within the Permanent Task-force after the establishment of the repository, which shall take no longer than 12 months.

ORE 31.3.1: Relevant Signatories will report on their work towards and contribution to the overall repository project, which may include (depending on the Signatories): financial contributions; technical support; resourcing; fact-checks added to the repository. Further relevant metrics should be explored within the Permanent Task-force.

Measure 31.4. Relevant Signatories will explore technological solutions to facilitate the efficient use of this common repository across platforms and languages. They will discuss these solutions with the Permanent Task-force in view of identifying relevant follow up actions.

ORE 31.4.1: Relevant Signatories will report on the technical solutions they explore and insofar as possible and in light of discussions with the Task-force on solutions they implemented to facilitate the efficient use of a common repository across platforms.

FACT-CHECKERS' ACCESS TO RELEVANT INFORMATION

Commitment 32. Relevant Signatories commit to provide fact-checkers with prompt, and whenever possible automated, access to information that is pertinent to help them to maximise the quality and impact of fact-checking, as defined in a framework to be designed in coordination with EDMO and an elected body representative of the independent European fact-checking organisations.

In order to satisfy Commitment 32:

Measure 32.1. Relevant Signatories will provide fact-checkers with information to help them quantify the impact of fact-checked content over time, such as (depending on the service) actions taken on the basis of that content, impressions, clicks, or interactions.

Measure 32.2. Relevant Signatories that showcase User Generated Content (UGC) will provide appropriate interfaces, automated wherever possible, for fact-checking organisations to be able to access information on the impact of contents on their platforms and to ensure consistency in the way said Signatories use, credit and provide feedback on the work of fact-checkers.

ORE 32.1.1 (for Measures 31.1 and 31.2): Relevant Signatories will provide details on the interfaces and other tools put in place to provide fact-checkers with the information referred to in Measure 31.1 and 31.2.

SLI 32.1.1 (for Measures 31.1 and 31.2): Relevant Signatories will provide quantitative information on the use of the interfaces and other tools put in place to provide fact-checkers with the information referred to in Measures 32.1 and 32.2 (such as monthly users for instance).

Measure 32.3. Relevant Signatories will regularly exchange information between themselves and the fact-checking community, to strengthen their cooperation.

ORE 32.3.1: Relevant Signatories will report on the channels of communications and the exchanges conducted to strengthen their cooperation - including success of and satisfaction with the information, interface, and other tools referred to in Measures 32.1 and 32.2 - and any conclusions drawn from such exchanges.

FACT-CHECKERS' STANDARDS

Commitment 33. Relevant Signatories (i.e. fact-checking organisations) commit to operate on the basis of strict ethical and transparency rules, and to protect their independence.

In order to satisfy Commitment 33:

Measure 33.1. Relevant Signatories will comply with the requirements of instruments such as being verified signatories of the International Fact-checking Network (IFCN) Code of Principles or the future Code of Professional Integrity for Independent European fact-checking organisations.

ORE 33.1.1: Relevant Signatories will report on the status of their membership to instruments such as those mentioned in Measure 33.1 and the actions taken as a result of that to ensure strict ethical and transparency rules, and to protect their independence.

SLI 33.1.1: Relevant Signatories will report on the number of European fact-checkers that are IFCN-certified or are members of the future Code of Professional Integrity.

VIII. TRANSPARENCY CENTRE

Whereas:

- (a) The Signatories recognise the key importance of transparency and accountability in the fight against online disinformation and the legitimate interest of the public to receive accurate and timely information about the implementation of the Code. Beyond their individual efforts to ensure the transparency of their respective services and products, Signatories therefore recognise the importance of a common point of reference and transparency with regard to the implementation of this Code.
- (b) Therefore, Signatories see the importance of establishing a common Transparency Centre website that is publicly available, user friendly, and searchable. They, therefore, agree to set up and finance the Transparency Centre website, to maintain it, and to keep it up to date with relevant information, including all quantitative metrics, in a timely and complete manner. Over time, Signatories will consider new state-of-the-art features or formats as relevant to the Transparency Centre's user base.
- (c) Signatories recognise the importance of the proper governance of the Transparency Centre website, which is to be overseen by the Task-force.

The Signatories of this Code commit to the following:

Commitment 34. To ensure transparency and accountability around the implementation of this Code, Relevant Signatories commit to set up and maintain a publicly available common Transparency Centre website.

In order to satisfy Commitment 34:

- Measure 34.1. Signatories establish and maintain the common Transparency Centre website, which will be operational and available to the public within 6 months from the signature of this Code.
- Measure 34.2. Signatories provide appropriate funding, for setting up and operating the Transparency Centre website, including its maintenance, daily operation, management, and regular updating. Funding contribution should be commensurate with the nature of the Signatories' activity and shall be sufficient for the website's operations and maintenance and proportional to each Signatories' risk profile and economic capacity.
- Measure 34.3. Relevant Signatories will contribute to the Transparency Centre's information to the extent that the Code is applicable to their services.
- Measure 34.4. Signatories will agree on the functioning and financing of the Transparency Centre within the Task-force, to be recorded and reviewed within the Task-Force on an annual basis.
- Measure 34.5. The Task-force will regularly discuss the Transparency Centre and assess whether adjustments or actions are necessary. Signatories commit to implement the actions and adjustments decided within the Task-force within a reasonable timeline.

Commitment 35. Signatories commit to ensure that the Transparency Centre contains all the relevant information related to the implementation of the Code's Commitments and Measures and that this information is presented in an easy-to-understand manner, per service, and is easily searchable.

In order to satisfy Commitment 35:

- Measure 35.1. Signatories will list in the Transparency Centre, per each Commitment and Measure that they subscribe to, the terms of service and policies that their service applies to implement these Commitments and Measures.
- Measure 35.2. Signatories provide information on the implementation and enforcement of their policies per service, including geographical and language coverage.

- Measure 35.3. Signatories ensure that the Transparency Centre contains a repository of their reports assessing the implementation of the Code's commitments.
- Measure 35.4. In crisis situations, Signatories use the Transparency Centre to publish information regarding the specific mitigation actions taken related to the crisis.
- Measure 35.5. Signatories ensure that the Transparency Centre is built with state-of-the-art technology, is user-friendly, and that the relevant information is easily searchable (including per Commitment and Measure). Users of the Transparency Centre will be able to easily track changes in Signatories' policies and actions.
- Measure 35.6. The Transparency Centre will enable users to easily access and understand the Service Level Indicators and Qualitative Reporting Elements tied to each Commitment and Measure of the Code for each service, including Member State breakdowns, in a standardised and searchable way. The Transparency Centre should also enable users to easily access and understand Structural Indicators for each Signatory.

Commitment 36. Signatories commit to updating the relevant information contained in the Transparency Centre in a timely and complete manner.

In order to satisfy Commitment 36:

- Measure 36.1. Signatories provide updates about relevant changes in policies and implementation actions in a timely manner, and in any event no later than 30 days after changes are announced or implemented.
- Measure 36.2. Signatories will regularly update Service Level Indicators, reporting elements, and Structural Indicators, in parallel with the regular reporting foreseen by the monitoring framework. After the first reporting period, Relevant Signatories are encouraged to also update the Transparency Centre more regularly.
- Measure 36.3. Signatories will update the Transparency Centre to reflect the latest decisions of the Permanent Task-force, regarding the Code and the monitoring framework.

QRE 36.1.1 (for the Commitments 34-36): With their initial implementation report, Signatories will outline the state of development of the Transparency Centre, its functionalities, the information it contains, and any other relevant information about its functioning or operations. This information can be drafted jointly by Signatories involved in operating or adding content to the Transparency Centre.

QRE 36.1.2 (for the Commitments 34-36): Signatories will outline changes to the Transparency Centre's content, operations, or functioning in their reports over time. Such updates can be drafted jointly by Signatories involved in operating or adding content to the Transparency Centre.

SLI 36.1.1 (for the Commitments 34-36): Signatories will provide meaningful quantitative information on the usage of the Transparency Centre, such as the average monthly visits of the webpage.

IX. PERMANENT TASK-FORCE

Whereas:

- (a) Signatories recognise the importance of setting up a permanent Task-force aimed at evolving and adapting the Code, including the ability to update its Commitments and Measures in view of technological, societal, market and legislative developments.
- (b) Signatories recognise the importance of participating in the Task-force with the goal of improving the effectiveness of the Code and its monitoring.
- (c) Signatories regard the Task-force as an important forum of exchange among Signatories, the Commission, the EEAS, ERGA, EDMO and other invited third-parties.

- (d) Signatories understand the importance of working in subgroups to implement specific workstreams in between the plenary meetings of the Task-force.
- (e) Signatories recognise the importance of involving relevant experts in the activity of the Task-force, and of organising exchanges with third-party stakeholders to keep them updated and gather their insights related to the disinformation phenomenon.
- (f) Signatories recognise the importance of assessing the impact and success of the Code of Practice against the spread of Disinformation. As such, within the first year of the Code's operations, Relevant Signatories will work together with the Task-force as well as with EDMO, ERGA, and relevant third-party experts to develop a first set of Structural Indicators that can help assess the impact and success of the Code. Signatories will then continue to work with the Task-force, EDMO, ERGA and relevant third-party experts to test and where necessary adjust these indicators over time.

The Signatories of this Code commit to the following:

Commitment 37. Signatories commit to participate in the permanent Task-force. The Task-force includes the Signatories of the Code and representatives from EDMO and ERGA. It is chaired by the European Commission, and includes representatives of the European External Action Service (EEAS). The Task-force can also invite relevant experts as observers to support its work. Decisions of the Task-force are made by consensus.

In order to satisfy Commitment 37:

Measure 37.1. Signatories will participate in the Task-force and contribute to its work. Signatories, in particular smaller or emerging services will contribute to the work of the Task-force proportionate to their resources, size and risk profile. Smaller or emerging services can also agree to pool their resources together and represent each other in the Task-force. The Task-force will meet in plenary sessions as necessary and at least every 6 months, and, where relevant, in subgroups dedicated to specific issues or workstreams.

Measure 37.2. Signatories agree to work in the Task-force in particular – but not limited to – on the following tasks:

- Establishing a risk assessment methodology and a rapid response system to be used in special situations like elections or crises.
- Cooperate and coordinate their work in special situations like elections or crisis
- Agree on the harmonised reporting templates for the implementation of the Code's Commitments and Measures, the refined methodology of the reporting, and the relevant data disclosure for monitoring purposes.
- Review the quality and effectiveness of the harmonised reporting templates, as well as the formats and methods of data disclosure for monitoring purposes, throughout future monitoring cycles and adapt them, as needed.
- Contribute to the assessment of the quality and effectiveness of Service Level and Structural Indicators and the data points provided to measure these indicators, as well as their relevant adaptation.
- Refine, test and adjust Structural Indicators and design mechanisms to measure them at Member State level.
- Agree, publish and update a list of TTPs employed by malicious actors, and set down baseline elements, objectives and benchmarks for Measures to counter them, in line with the Chapter IV of this Code.

- Seek out and discuss research, expert input and up-to-date evidence relevant to the Code's commitments, such as, *inter alia*, emerging best practices in safe design, retroactive flagging, repository of fact-checks, provenance tools.
- Discuss and provide guidance on the adequate quantitative information to be provided by signatories to fulfil their reporting obligations regarding agreements with fact-checking organisations across different services.
- Regularly discuss whether the Code's Commitments and Measures need updating in view of technological, societal, market and legislative developments, as well as in view of accommodating new signatories and, where the Task-force agrees to be necessary, carry out such updates.
- Review the appropriateness and consistency of adapted Measures for smaller or emerging services.
- Promote the Code among relevant peers and integrate new Signatories to the Code.

Measure 37.3. The Task-force will agree on and define its operating rules, including on the involvement of third-party experts, which will be laid down in a Vademecum drafted by the European Commission in collaboration with the Signatories and agreed on by consensus between the members of the Task-force.

Measure 37.4. Signatories agree to set up subgroups dedicated to the specific issues related to the implementation and revision of the Code with the participation of the relevant Signatories.

Measure 37.5. When needed, and in any event at least once per year the Task-force organises meetings with relevant stakeholder groups and experts to inform them about the operation of the Code and gather their views related to important developments in the field of Disinformation.

Measure 37.6. Signatories agree to notify the rest of the Task-force when a Commitment or Measure would benefit from changes over time as their practices and approaches evolve, in view of technological, societal, market, and legislative developments. Having discussed the changes required, the Relevant Signatories will update their subscription document accordingly and report on the changes in their next report.

ORE 37.6.1: Signatories will describe how they engage in the work of the Task-force in the reporting period, including the sub-groups they engaged with.

X. MONITORING OF THE CODE

Whereas:

- (a) Signatories recognise that the present Code requires a strong monitoring framework allowing to assess the implementation of the Code and the Code's impact in reducing the spread of disinformation online throughout the EU and including at the Member State level.
- (b) Signatories seek to implement a regular reporting and assessment mechanism of the implementation of the Code's Commitments, which should also indicate any pertinent changes to policies and actions.
- (c) Signatories acknowledge the importance of granular reporting and monitoring at EU and Member State level, to ensure the Code's efficient and consistent implementation throughout the EU.
- (d) Signatories regard the Transparency Centre and the Task-force as key instruments to provide transparency to the public and to review, adapt and improve the reporting and monitoring framework.
- (e) Signatories recognise that – as set out in the preamble - reporting obligations under the Code need to take into account the Signatories' size, the nature of their services and the resources available to them, making sure that they do not impose a disproportionate burden on providers of platforms that are not Very Large Online Platforms, as defined in the DSA.

The Signatories of this Code commit to the following:

Commitment 38. The Signatories commit to dedicate adequate financial and human resources and put in place appropriate internal processes to ensure the implementation of their commitments under the Code.

QRE 38.1: Relevant Signatories will outline the teams and internal processes they have in place, per service, to comply with the Code in order to achieve full coverage across the Member States and the languages of the EU.

Commitment 39. Signatories commit to provide to the European Commission, within 1 month after the end of the implementation period (6 months after this Code's signature) the baseline reports as set out in the Preamble.

Commitment 40. Signatories commit to provide regular reporting on Service Level Indicators (SLIs) and Qualitative Reporting Elements (QREs). The reports and data provided should allow for a thorough assessment of the extent of the implementation of the Code's Commitments and Measures by each Signatory, service and at Member State level.

In order to satisfy Commitment 40:

- Measure 40.1. Relevant Signatories that are Very Large Online Platforms, as defined in the DSA, will report every six-months on the implementation of the Commitments and Measures they signed up to under the Code, including on the relevant QREs and SLIs at service and Member State Level.
- Measure 40.2. Other Signatories will report yearly on the implementation of the Commitments and Measures taken under the present Code, including on the relevant QREs and SLIs, at service and Member State level.
- Measure 40.3. Signatories will regularly update the Transparency Centre with relevant QREs and SLIs, at least in line with their reporting period under this Code.
- Measure 40.4. Signatories will develop, within the Task-force, harmonised reporting templates.
- Measure 40.5. Signatories will regularly work to improve and optimise the monitoring and reporting framework of the Code, including the SLIs, within the Task-force, building in particular on feedback from the European Commission, ERGA and EDMO.

Measure 40.6. Signatories will cooperate with the European Commission, respond to its reasonable requests and provide the European Commission with reasonable information, data and further input necessary to assess the implementation of the Code, allowing for the Code's efficient and thorough monitoring, including at Member State Level.

Commitment 41. Signatories commit to work within the Task-force towards developing Structural Indicators, and publish a first set of them within 9 months from the signature of this Code; and to publish an initial measurement alongside their first full report. To achieve this goal, Signatories commit to support their implementation, including the testing and adapting of the initial set of Structural Indicators agreed in this Code. This, in order to assess the effectiveness of the Code in reducing the spread of online disinformation for each of the relevant Signatories, and for the entire online ecosystem in the EU and at Member State level. Signatories will collaborate with relevant actors in that regard, including ERGA and EDMO.

In order to satisfy Commitment 41:

Measure 41.1. Within 1 month of signing the Code, Signatories will establish a Working Group to tackle this objective. This working group will be tasked with putting forward data points to be provided by Platform Signatories, and a methodology to measure Structural Indicators on the base of these data points, to be executed by non-Platform Signatories. Signatories will share data points appropriate to enable the measurement of metrics to be determined by the working group, such as prevalence or other contextualised metrics for sources and spread of online disinformation. Signatories will assess the work that will be necessary to deliver on the goals of this commitment, and discuss within the Task-force whether financial support is required.

Measure 41.2. The Working Group will report on its progress to the Task-force on a trimestral basis. It will consult with expert stakeholders including but not limited to EDMO, ERGA, and researchers to inform its work and outputs. 7 months after the signing of the Code, a conference will be convened with external stakeholders to present on progress thus far and seek feedback.

Measure 41.3. By 6 months after the signing of the Code, the Working Group will table with the Task-force a workable proposal for such Structural Indicators. By 9 months, relevant Signatories will provide to others within the Working Group the data points required to measure the Structural Indicators, and they will share publicly the aligned Structural Indicators. The Working Group will publish their measurements for the Structural Indicators in line with the first full report by the Signatories, as well as its full methodology, with the understanding that those may still require refinements over time. Signatories commit to keep updating the measurements, aligned with their reporting periods. Measurements will be published on the Transparency Centre in a way that allow to monitor them over time for the entire ecosystem and between different services.

Commitment 42. Relevant Signatories commit to provide, in special situations like elections or crisis, upon request of the European Commission, proportionate and appropriate information and data, including ad-hoc specific reports and specific chapters within the regular monitoring, in accordance with the rapid response system established by the Task-force.

Commitment 43. Signatories commit to produce reports and provide data following the harmonised reporting templates and refined methodology for reporting and data disclosure, as agreed in the Task-force.

Commitment 44. Relevant Signatories that are providers of Very Large Online Platforms commit, seeking alignment with the DSA, to be audited at their own expense, for their compliance with the commitments undertaken pursuant to this Code. Audits should be performed by organisations, independent from, and without conflict of interest with, the provider of the Very Large Online Platform concerned. Such organisations shall have proven expertise in the area of disinformation, appropriate technical competence and capabilities and have proven objectivity and professional ethics, based in particular on adherence to auditing standards and guidelines.