Code of Practice on Disinformation – Report of Logically for the period January – December 2024

Table of Contents

Executive summary

Logically is a technology company that delivers powerful Artificial Intelligence and Machine Learning solutions to tackle the toughest modern information challenges. We have developed a suite of products to help government, trust and safety teams, and enterprises gain comprehensive insights into the increasingly complex information landscape. We also operate one of the world's largest fact-checking teams under our independent subsidiary, Logically Facts, which was created as a separate division in April 2023.

Our team of award-winning data scientists, engineers, analysts, developers and investigators possess deep domain expertise in the dynamics of misleading content, deceptive behaviour and harmful online narratives. The team is united by the company's mission to build advanced Artificial Intelligence to give organisations a decisive information advantage in combating threats online. Our OSINT team produces deep-dive investigations and reports on disinformation, including on foreign information manipulation and interference. Logically Facts publishes frequent indepth fact checks, in addition to more detailed analyses of particular developments.

Our Signatoryship to the EU Code of Practice on Disinformation allows us to contribute to the development and post-implementation monitoring of industry-drafted self-regulatory standards to fight threats to information integrity. We have opted into Commitments that are geared towards countering the tactics employed by online threat actors, boosting the impact of fact-checking operations and enhancing media literacy. This report will demonstrate how we adhere to those Commitments.

Commitment 14: This Commitment asks Signatories to outline the policies they have against the tactics, techniques and procedures (TTPs) employed by actors of disinformation. Logically does not provide a user-to-user service where such TTPs could manifest and so we do not have explicit policies against them. However, while we do not conduct policing actions against malicious actors, we do publish fact-checks and OSINT investigations that spotlight any TTPs employed, thereby providing case studies that can feed evidence-based policies by platforms or governments. The investigations we highlight in this report exemplify our identification of TTPs e.g. increased use of messaging platforms to control narratives as well as the amplification of content from fringe websites by hostile state actors.

Commitment 16: This Commitment asks Signatories to provide qualitative examples of cross-platform migration tactics employed by actors of disinformation to circumvent moderation policies, engage different audiences or coordinate action on platforms with less scrutiny. Logically's case studies demonstrate the way in which different kinds of disinformation actors migrated to different kinds of platforms depending on the kind of content they were looking to spread. For e.g., while *Telegram* and *Rumble* became new homes for far right extremists and Covid-19 conspiracy theories to begin disseminating content, climate misinformation began to be spread from blogging sites like *Substack* or *Medium*.

Commitment 17: This Commitment asked Signatories to report on the media literacy activities they undertook throughout the reporting period. Logically Facts partnered with TikTok to provide media literacy training which was accessible in several European countries and the UK ahead of elections. It also conducted a number of other media literacy initiatives in Sweden and the UK.

Commitment 29: This Commitment sought for Signatories to detail their methodologies for tracking and analysing influence operations and disinformation campaigns. In response, Logically cited the investigative methodologies employed in specified case studies, and detailed our work on ethical standards and data governance. We intend to keep our research

contributions updated in the Transparency Centre, including via annual reporting under the Code.

Commitment 30: This Commitment asked Signatories to report on actions to facilitate fact-checking organisations' cross-border collaboration. As a company with a dedicated fact-checking subsidiary, we have cited our involvement in the development of the European Fact-Checking Standards Network (EFCSN), our active cooperation with other organisations on specific fact-checks and subject matters, and our internal structural planning to prioritise such collaborations. We also demonstrated this commitment by participating in important events for the fact-checking community in 2024.

Commitments 31, 34, 35 and 36: These Commitments sought information on how Signatories are contributing to the development of a repository of fact-checking content, as well as the Transparency Centre. Logically intends to contribute to these as and when we are called upon by the Taskforce.

Commitment 33: In response to this Commitment to uphold ethical and transparency rules, we have cited our accreditation by the International Fact-Checking Network and our application to the EFCSN. We have also outlined our strict ethics and transparency policies, including our lists of prohibited clients and use cases, as well as the ways that we ensure our independence and non-partisanship.

Commitment 37: This Commitment asked about the Signatories' engagement with the Taskforce. Logically has remained steadfast in its engagement with the Taskforce. We continue to be part of four Subgroups, namely on the Empowerment of Fact-Checkers, the Integrity of Services, Generative AI, and on Elections.

Commitment 38: This Commitment called for Signatories to outline the internal teams dedicated to ensuring compliance with the Code. Logically has indicated the titles of the team members responsible for overseeing compliance, as well as the processes carried out. This included internal cross-functional consultations and reviews of internal documentation and policies.

2024 was a monumental year in Logically's growth. We have expanded the scope of our threat detection product, Logically Intelligence®. We developed a new tool, Logically Accelerate to assist fact checkers and journalists search and analyse short-form videos. We have carried out a number of media literacy initiatives and have increased our resources dedicated to this activity accordingly. As experts in our field, we can help government, trust and safety teams and enterprises to monitor and mitigate harmful information threats at speed and at scale and empower the public with accurate information to build societal resilience. We intend to continue expanding and refining these efforts in line with our Commitments under the Code in the next scheduled reporting round.

Guidelines for filling out the report

Reports are detailing how signatories have implemented their Commitments under the Code and 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.

Reporting period

The reporting period to be covered in the reports is 12 months (edit reporting period) for signatories who are not offering very large online platform services. Signatories shall submit reports outlining policy updates and actions taken to implement the Commitments and Measures they signed up to under the Code. All data and policy updates should be reported for 12 months period from the submission of last reports.

Adjusting the reporting template

Signatories who are not offering very large online platform services can adapt the template to specific commitments and measures they subscribed to. This may include adapted wording for commitments, measures, QREs and SLIs. Relevant signatories will report only on commitments and measures they subscribed to and provide Member State-level data only if feasible.

Reporting per Service

When filling in a report for several services, use colour codes to clearly distinguish between services. At the beginning of the report, clarify what colour is used for which service.

Reporting in text form

Reporting in the form of written text is required for several parts of the report. Most of them are accompanied by a target character limit. Please stick to the target character limit as much as possible. We encourage you to use bullet points and short sentences. When providing information to the QRE, please make sure that your answer covers all the elements of the associated commitment and measure. Links should only be used to provide examples or to illustrate the point. They should not be used to replace explanations or to provide data in the forms. All relevant explanations and data must be included in the report directly, in written form.

Reporting SLIs and data

Reporting on SLIs requires quantitative information to be reported on in this harmonised reporting template.

- Where relevant and feasible, SLIs should be reported on per Member State.
- If no data is available on Member State level, SLIs might, instead, be exceptionally reported on per language. (NB that signatories agreed to revisit this issue after the first reporting, to ensure harmonised and meaningful reporting.)
- Please report data in the format provided by the harmonised reporting template, not through external links. Please use the Member State/language template provided in the harmonised reporting template. Where the table asks for "Other relevant metrics", please name the metric that you would like to report on in addition to the ones already provided. You may include more than the number of additional fields provided where necessary; in that case, please adjust the table as needed.
- Please contextualize all data as much as possible, i.e. include baseline quantitative information that will help contextualize the SLIs (e.g. number of pieces of content labelled out of what volume of content).
- If there are no relevant metrics to report on, please leave the respective columns blank.

Reporting on TTPs

If subscribed to Commitment 14, Integrity of Services, we ask you to report on each identified TTP individually. The number of identified TTPs may vary per service. Where more than one TTP are reported under the same action, clarify the reasoning in the methodology. Where input is not provided, keep the placeholder for the relevant TTP and explain reasons and planned remedial action. Additionally, as with all other SLIs, data can be provided per Member State for each individual TTP.

Missing Data

In case that at the time of reporting there is no data available yet, the data is insufficient or the methodology is lacking, please outline in the dedicated field (i.e. in the field about further implementation measures planned) how this will be addressed over the upcoming six months, being as specific as possible.

Signatories are encouraged to provide insights about the data/numbers they provide by inserting possible explanations in the boxes of the template "*Methodology of data measurement & insights on data provided*". This should aim to explain the why of what is being reported, for instance - *Are there trends or curiosities that could require or use contextual explanation? What may be driving the change or the difference in the number?* Please also indicate inconsistencies or gaps regarding methodology in the dedicated box.

Attachments

We ask you not to enclose any additional attachments to the harmonised reporting template.

Crisis and elections reporting template

Relevant signatories are asked to provide proportionate and appropriate information and data during a period of crisis and during an election. Reporting is a part of a special chapter at the end of the harmonised reporting template and should follow the guidelines:

- The reporting of signatories' actions should be as specific to the particular crisis or election reported on as possible. To this extent, the rows on "Specific Action[s]" should be filled in with actions that are either put in place specifically for a particular event (for example a media literacy campaign on disinformation related to the Ukraine war, an information panel for the European elections), or to explain in more detail how an action that forms part of the service's general approach to implementing the Code is implemented in the specific context of the crisis or election reported on (for example, what types of narratives in a particular election/crisis would fall into scope of a particular policy of the service, what forms of advertising are ineligible).
- Signatories who are not offering very large online platform services and who follow the invitation to report on their specific actions for a particular election or crisis may adapt the reporting template as follows:
  - They may remove the "Policies and Terms and Conditions" section of the template, or use it to report on any important changes in their internal rules applicable to a particular election or crisis (for example, a change in editorial guidelines for fact-checkers specific to the particular election or crisis)
  - They may remove any Chapter Section of the Reporting Template (Scrutiny of Ads Placement, Political Advertising, Integrity of Services etc.) that is not relevant to their activities
- The harmonised reporting template should be filled in by adding additional rows for each item reported on. This means that rather than combined/bulk reporting such as "Depending on severity of violation, we demote or remove content based on policies X, Y, Z", there should be individual rows stating for example "Under Policy X, content is demoted or removed based on severity", "Under Policy Y, content [...]" etc.
- The rows should be colour-coded to indicate which service is being reported on, using the same colour code as for the overall harmonised reporting template.

Reporting should be brief and to the point, with a suggested character limit entry of 2000 characters.

Uploading data to the Transparency Centre

The reports should be submitted to the Commission in the form of the pdf via e-mail to the address CNECT COP TASK FORCE CNECT-COP-TASK-FORCE@ec.europa.eu within the agreed deadline. Signatories will upload all data from the harmonised reporting template to the Transparency Centre, allowing easy data access and filtering within the agreed deadline. It is the responsibility of the signatories to ensure that the uploading takes place and is executed on time. Signatories are also responsible to ensure that the Transparency Centre is operational and functional by the time of the reports' submission that the data from the reports are uploaded and made accessible in the Transparency Centre within the above deadline, and that users are able to read, search, filer and download data as needed in a user-friendly way and format.

IV. Integrity of Services

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 following TTPs pertain to the creation of assets for the purpose of a disinformation campaign, and to ways to make these assets seem credible:
- 1. Creation of inauthentic accounts or botnets (which may include automated, partially automated, or non-automated accounts)
- 2. Use of fake / inauthentic reactions (e.g. likes, up votes, comments)
- 3. Use of fake followers or subscribers
- 4. Creation of inauthentic pages, groups, chat groups, fora, or domains
- 5. Account hijacking or impersonation

The following TTPs pertain to the dissemination of content created in the context of a disinformation campaign, which may or may not include some forms of targeting or attempting to silence opposing views. Relevant TTPs include:
- 6. Deliberately targeting vulnerable recipients (e.g. via personalized advertising, location spoofing or obfuscation)
- 7. Deploy deceptive manipulated media (e.g. "deep fakes", "cheap fakes"...)
- 8. Use "hack and leak" operation (which may or may not include doctored content)
- 9. Inauthentic coordination of content creation or amplification, including attempts to deceive/manipulate platforms algorithms (e.g. keyword stuffing or inauthentic posting/reposting designed to mislead people about popularity of content, including by influencers)
- 10. Use of deceptive practices to deceive/manipulate platform algorithms, such as to create, amplify or hijack hashtags, data voids, filter bubbles, or echo chambers
- 11. Non-transparent compensated messages or promotions by influencers
- 12. Coordinated mass reporting of non-violative opposing content or accounts

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.

QRE 14.3.1	*Signatories will report on the list of TTPs agreed in the Permanent Taskforce within 6 months of the signing of the Code and will update this list at least every year. They will also report on the common baseline elements, objectives and benchmarks for the policies and measures. They will also update the Transparency Centre with this information.*
	Outline relevant actions [suggested character limit: 2000 characters]:
	Logically Facts and Logically publish fact-checks and open-source intelligence (OSINT) investigations, respectively, to counter threat actors' manipulative tactics, techniques and procedures (TTPs). As we do not conduct any policing actions, we do not have formal policies in place to address these. However, our publications can educate audiences on such TTPs, and equip stakeholders with the case studies needed to feed evidence-based policies.
	Logically became a member of the Subgroup on the Integrity of Services in September 2023, and has subsequently attended and contributed to several meetings in the regular review of the list of TTPs.
	Examples of identified TTPs
	Narrative control through messaging platforms and subsequent migration
	In February 2023, we [identified](#) a French-language, cross-platform network targeting Africa being run by individuals affiliated with the Russian Government and uncovered "fringe actors" associated with the operation. In February 2024, we conducted [further investigations](#) into the network and found a particular member's attempts to establish independence campaigns within the United States, with the backing of the Russian Government and PMC Wagner.
	In September 2024, we [conducted further investigations](#) into the network. Logically assessed that the identified member, Andre Dembele, made a public Telegram channel private, detailing unprecedented levels of encrypted communications with individuals working in Russia and West Africa, members of PMC Wagner, and individuals affiliated with a bank operating an office in UK.
	(For more details on migration tactics including the use of Telegram, please see the response to QRE 16.2.1 below)
	Amplification of fringe sites for strategic objectives by hostile state actors

- During the course of the violence in the United Kingdom in July and August 2024 that followed the tragic knife attack in Southport, Logically and Logically Facts published a number of reports assessing the spread of disinformation regarding the identity of the attacker. We identified a bogus news website, "Channel 3NOW" which published the supposed name of the attacker as part of an article that was then later cited by Russian state media as a source and amplified. The website's details – such as its registrant being located in Lithuania while being based out of Pakistan and its regular cycling through another bogus news branding – and the flow of information in and out of the website resembles Russian approaches around information laundering and narrative dissemination. While it cannot be proven that "Channel 3NOW" was part of a larger foreign interference effort, its use by Russian state media to increase the circulation of disinformation that increased inter-ethnic tensions in the UK meant it functioned in a way advantageous to hostile states.

Non-transparent compensated messages or promotions by influencers

- In March 2023, Logically carried out an investigation into the Russian "fact-checking" website "War on Fakes". We were able to attribute the website to Timofey Vasiliev, a former Russian journalist who had not disclosed that he was a Russian state television presenter with widespread relationships to Russian influencers with over 1 million followers who promoted the page during its initial creation.
- To conduct attribution, we reviewed changes that were made on the "WHOIS" registry of public available information about a given domain. The details on the site's registration could be connected to War on Fakes, Vasiliev, and his ties to the Russian government and propagandist community. We made this connection by reviewing the name, phone number and email address of the corresponding accounts. A review of Vasiliev's career dating back to 2011 also revealed several roles where Vasiliev was a known affiliate of groups associated with Russian propaganda e.g. the Russian propaganda outlet Ridus. We found information on his resume in the archive of his personal website, as well as through career histories available on the websites of organisations that Vasiliev has worked for.
- Logically further identified two other initiatives that Vasiliev was actively engaged with at the time of our investigation – Klub5000 and SVO. The former sought to bring together monthly donors to vetted Russian military and civilian causes, and offered potential trips to the "Special Operation Zone". The latter provided twice daily news updates of the biggest stories from the Russian government and the war in Ukraine. Given the lack of disclosure on the website about Vasiliev's background, this can be considered a non-transparent promotion by an influencer.

Internal processes to better identify TTPs

	As we reported in our Baseline Report of January 2023, we are also developing an end-to-end automated Coordinated Inauthentic Behaviour (CIB) identification system as part of our disinformation detection and reporting service, Logically Intelligence®, to assist human experts. The development of this system is progressing, and has been deployed to support OSINT experts delivering on commercial projects. Further plans to improve the CIB system's efficacy through active learning are in progress.
	We are also undertaking research on how to approach the detection of foreign information manipulation and interference via data science and machine learning. We aim to create a system that can be deployed alongside our expert teams. The deployment of this system would be governed by our 'Human and Machine in the Loop Evaluation and Training' (HAMLET) framework, which is intended to maximise machine-learning techniques by maintaining a human-in-the-loop capability.

IV. Integrity of Services	
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.	
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.
QRE 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.* *Outline relevant actions [suggested character limit: 2000 characters]:* Misinformation actors adapt to moderation by shifting platforms, masking chatter - including the utilisation of written languages foreign to themselves, and exploiting policy gaps. This behavior is

highly likely to persist as enforcement evolves and technologies shift. Key examples include:

- **Covid-19 Misinformation**. Anti-vaccine groups, facing restrictions on *Facebook* and *YouTube*, almost certainly [migrated to *Telegram and Rumble*](#), using coded language to bypass moderation.

- **QAnon Rebranding**. Following their deplatforming in 2020, QAnon affiliates effectively rebranded as child protection advocates and [moved](#) to *Gab*, *Parler*, and *Telegram*.

- **4chan**. The forum [remains an attractive haven](#) for hostile actors to migrate to once they have engaged with specific online communities. Boards such as /pol/ (politically incorrect) generate and refine extremist, conspiratorial, or harmful narratives, which become "ops" (operations), where users craft misleading or provocative messages, which then become memes, slogans, or fake news in order to make the narrative more shareable on mainstream social media.

- **State-Backed Disinformation**. Russian actors [highly likely shifted](#) from *Facebook* to encrypted apps such as *Telegram* and fringe forums, using AI-generated personas. Cross-pollination has been observed between *ok.ru*, *Telegram*, and *X*.

- **Far-Right Extremism**. After January 6th, groups such as the Proud Boys [migrated](#) to *Rumble* and *Telegram*, likely seeking to exploit weak moderation.

- **Climate Misinformation**. Climate denialists [likely moved to *Substack* and *Medium*](#), then used mainstream platforms to distribute misleading content.

Recommendations for the UK Government and Relevant Signatories

- **Cross-Partner Intelligence Sharing**. UK agencies, tech firms, and fact-checkers should collaborate on tracking migration patterns, and share intelligence on threat actor TTPs in order to identify and disrupt narrative migration.

	● **Behavioural Analysis**. Encourage platforms to detect patterns of evasion, including [coded language](#), proxy accounts, or inauthentic behaviours.
	● **Public Awareness**. Publish regular reports on hostile information campaign tactics to improve digital resilience, as well as run media literacy campaigns.
	● **Stronger Platform Accountability**. Encourage standardised moderation policies and transparent enforcement across traditional and social media platforms.
	● **Policy Adjustments**. Identify and close regulatory loopholes to ensure coverage of less-regulated platforms, or websites masquerading as local media sources.

V. Empowering Users	
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.	
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.
QRE 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.* Logically Facts partnered with TikTok to feature media literacy videos on their EU election hubs for Ireland, Sweden, Finland, Denmark, Cyprus, Slovenia, Estonia, Malta and Latvia, in order to better prepare users to identify misinformation during the European elections. Redirection to these hubs was triggered by keyword searches related to the elections. Once triggered, users' interface would point them to credible sources of

information, as well as media literacy videos produced by Logically Facts. Crucially, these videos corresponded to the relevant EU language(s) for each of the aforementioned Member States. The Danish example can be found here.

Logically Facts also partnered with TikTok to feature media literacy videos in the UK for the local elections in May and the general elections in July to help users on how to spot and counter misinformation. More info here for the general election hub and for the local election here

In 2024, Logically Facts' fact-checkers led some courses on how to verify information online organised by the Swedish media institute Fojo:

A course called "Go Verify! How to become a professional fact-checker" with Fojo Media Institute for the Swedish section of Yle in Helsinki, Finland. The course, conducted between March 4 and 6, 2024, taught participants how to do fact-checks, how to use digital verification tools, and how disinformation is spread.

In April 2024, we held a training workshop about TikTok for the Swedish anti-racism magazine EXPO in Stockholm, Sweden. We covered security, how the app works and its features, how we can use the algorithm to our advantage, and specifically, how you can do investigations on the app.

A fact-checker from Logically Facts conducted a three-day fact-checking course with Fojo Media Institute in Kalmar, Sweden, between September 3 and 5, 2024, titled "Verify this—How to become a professional fact checker."

In November, our Swedish fact-checkers were in Kalmar at the Swefactcheck conference "Media, power, and manipulation in a time of Generative AI," organized by the Fojo Media Institute. They led a session called "Fact-checking the Super election year: Our experiences and conclusions."

The head of Editorial Operations in UK and Europe was invited as a guest lecturer at City University in London in November to talk about how to use social media platforms as news gathering sources and how to fact-check the content online.

The Editorial team of Logically Facts has contributed to a series of ethical journalism training programs that Impress, an independent press regulator in the UK, is putting together for the public. We have been interviewed for the topics on mis and disinformation, fake news and social media, disability and principles of ethical reporting.

SLI 17.2.1 – actions enforcing policies above	*Relevant Signatories report on number of media literacy and awareness raising activities organised and or participated in and will share quantitatiN ve 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).*

	Methodology of data measurement: [suggested character limit: 500 characters]:				
	Nr of media literacy/ awareness raising activities organised/ participated in:	*Reach of campaigns:*	*Nr of participants:*	*Nr of interactions with online assets:*	*Nr of participants (etc):*
Data	Articles on media literacy				
	Media literacy videos (Ireland, Sweden, Finland, Denmark, Cyprus, Slovenia, Etonia, Malta and Latvia)			Number of views: 47M	
	4 courses/workshops on how to fact-check		73 in total		
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.				
QRE 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.*** Logically Facts has worked very closely with the [Fojo Media Institute](#) in Sweden to conduct courses to help journalists fact-check content online.				

VI. Empowering the research community

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.

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.*** *Outline relevant actions [suggested character limit: 2000 characters]* **Ethical Standards** Logically is one of the founding members of ObSINT, the European Open Source Intelligence Organisations Observatory. This organisation sets out common guidelines and best practices for OSINT practitioners, with a view to enhancing the community's collective capacity to produce accurate, ethical, and relevant information. Further information about our ethics policies can be found elaborated in our response to Commitment 33 of this Code
QRE 29.1.2	***Relevant Signatories will update their research in the Transparency Centre to allow for greater awareness and availability of their work.*** *Outline relevant actions [suggested character limit: 2000 characters]*

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.* *Outline relevant actions [suggested character limit: 2000 characters]* We have circulated relevant information on the methodology used for our investigations in more detail to the Taskforce via the Commission, and intend to keep the Taskforce informed of research activities we conduct that are of relevance, and the associated methodologies via our annual reporting. Logically already publishes information on its investigations carried out on our website (https://logically.ai/research).
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.* *Outline relevant actions [suggested character limit: 2000 characters]* Logically has not conducted research into the effectiveness of resilience-fostering measures on platforms (e.g. labels, warnings, ex-post notifications). As noted in our previous annual report for January to December 2023, this falls outside of our scope of work, and we intend to withdraw from this Measure of the Code. Should the scope of our research change in the future, we intend to re-subscribe to this Measure. However, as it currently stands, we have no way of determining the effectiveness of labels or warnings on platforms, as this is data that only the platforms themselves would have. We also cannot make this assessment for content classification conducted on our threat detection product, Logically Intelligence®, as we do not have oversight of how users utilise information found on Logically Intelligence®
SLI 29.2.1	*Relevant Signatories will report on the reach of stakeholders or citizens informed about the outcome of their research projects.* *Methodology of data measurement: [suggested character limit: 500 characters]*

	Reach of stakeholders or citizens informed about the project:

VII. Empowering 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.

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.
QRE 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.*** *Outline relevant actions [suggested character limit: 2000 characters]* Logically Facts is committed to following the principles promoted by the European Fact-Checking Standards Network, an EU-backed effort to create a Code of Professional Integrity for fact-checkers across the continent"
Measure 30.3	Relevant Signatories will contribute to cross-border cooperation between fact-checkers.
QRE 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.*** *Outline relevant actions [suggested character limit: 2000 characters]*

	Logically Facts became a member of EDMO in February 2024 and since then we have provided data and information about our fact-checks to contribute to their monthly fact-checking briefs. They can be found [here]().
	Logically Facts participated in the EU Disinfo Lab summit in Latvia, the GlobalFact 11 in Sarajevo, the EDMO conference in Belgium, among others, to connect and discuss with fact-checking organisations, policy makers, and experts in Europe and around the world ideas, challenges and projects in the mis/disinformation space.
	Managing Director Baybars Orsek participated in GlobalFact 11's panel discussion about the future of fact-checking in the rapidly evolving landscape on June 28, 2024.
	Logically Facts attended a [panel discussion]() on October 8, 2024, hosted by the European Commission Representation in Ireland and European Movement Ireland on disinformation trends in the EU and Ireland covering challenges of mis/disinformation on civil society, elections, and EU institutions and policies.
	One of our fact-checkers spoke at a panel discussion on September 17, 2024, on EU-related disinformation during the EU Days in Lund, Sweden, called "The Battle for Truth: Addressing Disinformation in EU Election Coverage." She discussed lessons learned and whether new methods can be applied to future elections to ensure election security.
	Logically is also a member of the Subgroup on the Empowerment of Fact-Checkers under the EU Code of Practice, represented by the Managing Director of Logically Facts - see our response to Commitment 37 for more information on how we engaged in the work of the Taskforce, including the Subgroups we engaged with.

VII. Empowering the fact-checking community
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.

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.
QRE 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.* *Outline relevant actions [suggested character limit: 2000 characters]* We look forward to contributing to the repository as and when we are called upon to do so by the Taskforce.
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.
QRE 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.* *Outline relevant actions [suggested character limit: 2000 characters]* We look forward to contributing to the repository as and when we are called upon to do so by the Taskforce.

VII. Empowering the fact-checking community
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.

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.
QRE 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.*** *Outline relevant actions [suggested character limit: 2000 characters]* **IFCN & EFCSN** Logically Facts has filed its applications for renewal and grant of verified signatory status with the IFCN and the EFCSN. Its website includes information consistent with their codes of principles, including on <u>transparency of methodology</u> as well as <u>transparency of funding and non-partisanship</u>. **Ethics & Transparency** Logically and Logically Facts are both bound by Logically's Ethics Charter, which includes commitments to non-partisanship in line with the Code of Principles of the IFCN. The Charter prohibits contracting with certain kinds of customers including political parties and organisations, as well as use cases such as unlawful surveillance. Logically Facts has also adopted by-laws to cement its editorial independence from other parts of the organisation, and enforce its non-partisanship policy (these can be found at the end of the Ethics and Transparency page <u>here</u>).

VIII. Transparency Centre
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.

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.

VIII. Transparency Centre
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.

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.

VIII. Transparency Centre	
Commitment 36 Signatories commit to updating the relevant information contained in the Transparency Centre in a timely and complete manner.	
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.** Outline relevant actions [suggested character limit: 2000 characters] We contribute to the Transparency Centre as and when we are called upon to do so by the Taskforce. We publish our annual reports on time on the Transparency Centre website and use these to follow up on our original baseline report by outlining any updates relevant to our Commitments.
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.** Outline relevant actions [suggested character limit: 2000 characters]
SLI 36.1.1 – (for Measures 34 and 36)	**Signatories will provide meaningful quantitative information on the usage of the Transparency Centre, such as the average monthly visits of the webpage** Methodology of data measurement: [suggested character limit: 500 characters]
	Our company would like to provide following data:
Data	

IX. Permanent Task-Force

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.	
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.

QRE 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.***
	
	Outline relevant actions [suggested character limit: 2000 characters]
	
	We joined the Working Group on Elections, represented by our Head of UK/EU Fact-Checking. This involved:
	    ● Attending our Working Group Meetings from January to December 2024.
	    ● Contributing to the review of the template for reporting on elections and the Rapid Response System (RRS).
	    ● Attending RRS election meetings.
	
	We continued to be part of the Subgroup on the Integrity of Services, represented by our Director of AI Research and
	Solutions. This involved:
	    ● Attending Subgroup meetings;
	    ● Monitoring for new tactics, techniques and procedures (TTPs) that should be accounted for in
	    ● the obligations set out in Commitment 14.
	
	We continued to be part of the Subgroup on the Empowerment of Fact-Checkers, represented by Logically's Vice-President of Fact-Checking, who is also Managing Director of Logically Facts. This involved:
	    ● Attending Subgroup meetings;
	    ● Contributing to discussions on the governance side of the proposed repository of fact-checking content.

	We had also been part of the Subgroup on Generative AI as a co-chair, represented by our Senior Government Affairs Manager for the EU and UK.

X. Monitoring of Code

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 38.1.1 | **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.**

 Outline relevant actions [suggested character limit: 2000 characters]

 We have maintained the number of team members co-authoring this report and overseeing Logically's overall compliance with the Code since the publication of our previous report. The designated staff with these responsibilities have been:
 • The Senior Government Affairs Manager (EU/UK)
 • The Senior Corporate Affairs Manager (Global)
 • The Director of AI Research and Solutions
 • The Head of UK/EU Fact-Checking
 • The Global Head of Fact-Checking
 • The Vice-President of Fact-Checking

 Our internal processes to ensure compliance with the Code included:
 • Verification of documentation on the company's communal Google Drive and Confluence workspaces (particularly the folders relating to our applications to and status as a verified signatory of the
 • International Fact-Checking Network (IFCN)) to ascertain existing compliance;
 • Organising meetings with the European Commission to confirm our understanding of how to contribute to the work of relevant Subgroups;
 • Integrated systematic collaboration between the Corporate Affairs team and Logically Facts via |

	monthly coordination meetings; • Liaising with Logically's OSINT investigators and Logically Facts' editorial teams to obtain the research methodologies and outcomes required to fulfil Commitments 14, 16 and 29; • Updating the company's ethics and transparency policies and implementing new by-laws for Logically Facts; • Maintaining compliance with the IFCN Code of Principles, which is compatible with the requirements of Commitment 33. All Logically staff are trained in our ethics and transparency policies upon commencing their employment, and all ethics and transparency processes are documented on the company's shared online workspace.

X. Monitoring of Code
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.

X. Monitoring of Code
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.

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.

X. Monitoring of Code
Commitment 43
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 Taskforce.