Code of Practice on Disinformation – Report of Logically for the period January – December 2023

Table of Contents

IV. Integrity of Services	1
Commitment 14	1
Commitment 16	3
V. Empowering Users	5
Commitment 17	7
Commitment 29	8
VII. Empowering the fact-checking community	12
Commitment 30	12
Commitment 31	14
Commitment 33	15
VIII. Transparency Centre	18
Commitment 34	18
Commitment 35	19
Commitment 36	20
IX. Permanent Task-Force	21
Commitment 37	21
X. Monitoring of Code	23
Commitment 38	23
Commitment 39	24
Commitment 40	24
Commitment 43	25
Reporting on the service's response during a period of crisis	26
War of aggression by Russia on Ukraine	26
Israel-Hamas conflict	29
Reporting on the service's response during an election	32
European Elections 2024	32

Executive summary

Logically is a technology company that combines advanced artificial intelligence (AI) with world-class open-source intelligence (OSINT) investigators to uncover and address harmful misinformation and disinformation at speed and at scale. We have developed a suite of products and services to help government bodies, businesses and social media platforms reduce the real-world harms that can derive from the spread of misinformation and disinformation campaigns. We also operate one of the world's largest fact-checking teams under the independent subsidiary, Logically Facts, which was created as a separate division in April 2023.

Our award-winning data scientists, engineers, analysts, developers and investigators are united by the company's mission to enhance civic discourse, protect democratic debate and process, and provide access to trustworthy information. Our OSINT teams produce deep-dive investigations and reports on specific misinformation, disinformation and malinformation trends. Logically Facts publishes frequent 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 disinformation. We have opted into Commitments that are geared towards countering the tactics employed by disinformation 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. the creation of inauthentic pages in the form of fake news websites. We also identified an increased risk of deceptive manipulated media being created for disinformation as a result of the democratisation of generative AI tools.

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 attempts to mutually reinforce an actor's presence on separate platforms, and the reposting of content between mainstream platforms and those that are more fringe.

Commitment 17: This Commitment asked Signatories to report on the media literacy activities they undertook throughout the reporting period. Logically Facts reached important milestones in 2023 to strengthen its efforts in this area, producing regular media literacy content, providing training to journalists and partnering with TikTok to raise awareness of harmful misinformation in Sweden and Finland. Logically Facts also rolled out a series of educational videos in TikTok's app that shared tips on how to detect and counteract incorrect and misleading information.

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 2023.

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's engagement with the Taskforce has increased significantly since the last reporting round. We have ramped up our contributions to Taskforce Plenary sessions, having delivered presentations on the impact of AI on the disinformation landscape at both plenary sessions held in 2023. We have also joined 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.

2023 was a key year in Logically's growth. We have narrowed the scope of our threat detection product, Logically Intelligence[®], to election integrity and national security use cases. 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 public authorities and platforms to monitor and mitigate harmful misinformation and disinformation 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 disinformation 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 is therefore now a contributor in the regular review of the list of TTPs.
	Examples of identified TTPs
	 Creation of inauthentic pages, groups, chat groups, fora, or domains In February 2023, we identified a French-language, cross-platform network sharing Russian disinformation focusing on anti-colonial narratives. Based on domain analysis, we were able to attribute this network to Luc Michel, a self-proclaimed political activist connected to the Wagner Group. The network has engaged in influence operations in Africa since 2011, including via fake news websites masquerading as local news that we identified through manual assessment. The Eurasian Observatory for Democracy & Elections which is run by Luc Michel also organised the "observers" for the referenda in Crimea and Donbas.
	 Deploy deceptive manipulated media (e.g. "deep fakes", "cheap fakes") In July 2023, Logically tested three image-based generative AI platforms to see if they would produce evidence of false election-related narratives. More than 85% of prompts were accepted with little to no content moderation. In the UK, a key narrative is about the issue of immigration. Using Stable Diffusion, DALL-E 2 and Midjourney, Logically was able to generate images of hundreds of people arriving across the English Channel. Though the images produced were of only moderate quality, prior precedent has shown that even poor-quality images can still be used in malicious capacities e.g. Russia Today amplified the AI-generated image of an alleged explosion at the Pentagon in May 2023. By "flooding the zone" with an overload of false content, malicious actors can confuse audiences and sow distrust. The lack of safeguards on multimodal generative AI platforms against such use could pose a significant threat to global elections in 2024, by enhancing the ability to deploy deceptive manipulated media that can form part of disinformation campaigns.
	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

influence operations, foreign interference in information s	nge between their relevant teams in order to proactively share information about cross-platform pace and relevant incidents that emerge on their respective services, with the aim of preventing liance 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]:
	We regularly publish information on our websites to reach fellow Signatories and other stakeholders. The case studies below qualitatively demonstrate the tactic of cross-platform migration to engage diverse audiences. In this way, malicious networks can mutually reinforce their cross-platform presence and engage users on more fringe platforms where content moderation may be applied to a lesser extent.
	 Logically's monthly assessments of the top Russian disinformation narratives in Q1 2023 (January; <u>February</u>; <u>March</u>) revealed a targeting of Ukraine across different platforms by explicitly Russian state-owned or -aligned accounts. We initially identified the top narratives on Telegram based on their reach, and subsequently tracked them crossing over to VKontakte and X where they could acquire broader audiences. We were able to observe this cross-platform migration by virtue of the direct citations of these Russia-aligned channels on different platforms.
	• In February 2023, Logically <u>identified</u> a French-language, cross-platform network called either "Russosphere" or "En Defense de la Russie", which shared Russian disinformation focusing on anti-colonial narratives. A YouTube channel was created in November 2021, and an associated X profile went live three days before Russia's invasion of Ukraine in February 2022. Across these platforms, as well as Facebook and Telegram, "Russosphere" accounts gained more than 78,000 followers and subscribers since the first account was created. We were able to isolate the different channels across these platforms by cross-referencing their usernames, bios and profile pictures.

	• In May 2023, Logically Facts investigated a YouTube channel called "A Call for An Uprising" (Call) spreading conspiracies and disinformation about COVID-19, vaccines, 5G, and climate change. We first discovered Call on Twitch, and learned from other YouTubers that that at least eight alternate accounts were run alongside the main channel. Call's tactic was to create "gaming" channels, and to then switch back to conspiracy content once the a monetization threshold was reached. The alternate channels were banned upon the accumulation of around 80k subscribers, but Call then proceeded to create two new YouTube channels and a Rumble channel. Call also used a "self-destruct" approach to evade YouTube's policies and remain undetected, where videos are deleted a few days after being uploaded. This tactic aims to "game" the platform's rules by removing violative content before it can be found and cause the channel to be suspended. Call's tactics demonstrate a broader problem of adaptation to evade moderation.
--	--

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 started to produce regular media literacy content in April 2023, with articles and videos supported by social media videos and posts. Some examples are 'How to fact-check when news is breaking, A guide to detecting AI-generated images', and 'A guide on reading beyond the headlines' to help people make an informed judgement about the real facts. This content was also adapted and published across our social media channels on TikTok, Instagram, YouTube and Facebook to increase our reach. As a part of a video pilot project with TikTok, Logically Facts published media literacy videos on the platform to cover the topics stated above among others, such as explaining 'Why we are susceptible to online misinformation', 'How to geolocate a video or image', and sharing 'Three steps to help people stop sharing misinformation'. 		

	elections in the UK in It pointed users to cr produced on ' <u>How to</u> when viewing and in Logically Facts further information hubs on through the search o produced by Logical a guide on AI-genera Also in December 20 fact-checking togeth course was commiss Sweden with the too In 2024, Logically Fac fact-checking and di	May 2023. The interview of May 2023. The interview of the sources of information of the spot misinformation of the spot misinformation of the spot misinformation of the spot misinformation of the spot of the sp	ention was triggered b mation with a link to a online' and reminded u -related content. This k in December 2023 o sh hub link, Finnish hub media literacy topics. T vedish, 3 videos in Finr ng beyond the headlind acts' fact-checkers co- bedia institute Fojo and Civil Contingencies Ag ims and uncover misin edia Literacy officer to to create a bank of or	organised a <u>three-day</u> freelance journalist Jou gency and provided jou formation. provide expert guidand nline training videos an	lated to the elections. that Logically Facts Community Guidelines m 26 April to 1 June. sisted of in-app faced to users ational videos uch as lateral reading, <u>intensive course</u> in nathan Lundberg. The urnalists from all over ce and training in the d modules.
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 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). 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	1 media literacy campaign on the UK local elections in May 2023 with TikTok	112 users read the article		235 views	

	6 media literacy videos for a campaign in Sweden and Finland in December 2023 with TikTok			Swedish videos had over 8 million views (as of 1 February 2024) Finnish videos had over 9 million views (as of 1 February 2024)	
	Training with journalists in Sweden in December 2023		20		
Measure 17.3	implementation, and literacy experts in the Media Literacy Action organisations that ha	impact measurement e EU, including, for inst n Group, EDMO, its con ve relevant expertise.	of tools, relevant Signa ance, the Commission untry-specific branche	rtise of media literacy atories will partner or c 's Media Literacy Expe s, or relevant Member	onsult with media rt Group, ERGA's State universities or
QRE 17.3.1	purposes of all Meas Logically Facts has pr and be better prepar a media literacy expl US President Donald elections in the UK in the UK' and 'Types of When we create com include the Internation co-founder of the inv Commission, among Logically Facts has al work together on sev	roduced media literacy ed in case they come a ainer on ' <u>How to detec</u> Trump went viral. We May 2023 e.g. ' <u>Electic</u> f misinformation you sh tent like this, we reach onal Fact-Checking Ner vestigative journalism p others. so consolidated a netw veral projects, such as	ent. v explainers and prebu- across misinformation act Al-generated image: also created several pons bould not fall for during hould not fall for during n out to subject matter twork's community and blatform, Bellingcat, Eli- vork with the Fojo Med having one of our loca	nks for people to have on relevant topics. For s' when the images of rebunks and explainer isinformation online for g Election Day in the U experts to provide the d impact manager Eno ot Higgins, and the UK lia Institute in Sweden. I fact-checkers provide es to apply for projects	reliable information example, we created The Pope and former s ahead of the local <u>the local elections in</u> <u>K</u> . ir input. These ck Nyariki, the Electoral We partnered to e fact-checking
	opportunities togethe	er to further our joint ir	nterests in the area of f	es to apply for projects act-checking and activ particular focus on the	e collaboration

journalistic methods and raising awareness as well as increasing capacity-building and resilience among
media enterprises and newsrooms in Sweden and across Europe.

	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.		
	Data Governance		
	 Similarly to other open-source intelligence organisations, to carry out our work we ingest open-source public domain data from third-party data brokers and other public sites that collectively meet the accepted definition of "Publicly Available Information" under EU Regulation 2016/679, the General Data Protection Regulation (GDPR), and other national jurisdictions e.g. the California Privacy Act of 2023. Some public domain data ingested (e.g. individual user names on social media) is defined by GDPR, as 'personal data'. 		

 Logically has Standard Operating Procedures (SOPs) when its practitioners uncover personal data, its use and its storage, and we further adhere to our own ethics policy in addition to the provisions of the GDPR associated with processing personal data. When assessing malicious actors' tactics, techniques and procedures, and reporting our findings, Logically's SOPs govern methods of redaction, pseudonymisation and full anonymisation of personal data. SOPs for document storage, document labelling also have access controls to limit the employee(s) working on a research project for the purposes of data minimisation. Logically does not surveil any individual or group without due legal authority. Our SOPs outline that no research may be undertaken if it amounts to surveillance as defined within the UK Regulation of Investigatory Powers Act (2012) or similar investigatory powers in the EU. Logically researchers cannot be instructed or authorised to conduct research without due legal authority under this legislation. The requesting entity must have such powers within the jurisdiction they operate in or be explicitly exempt (such as in cases of national security and public safety). We adopt a defence-in-depth strategy when it comes to network security i.e. we employ a layered approach from physical security, through to data security. Data to and from our public websites (www.logically.ai and www.logicallyfacts.com) is encrypted in transit and at rest, by default. We use Role-Based Access Controls and adopt the principles of Least Privilege and Need To Know to manage access to data. Whether for our own research or for client work, we have formal SOPs for data retention policies, including the deletion of all extraneous data and the retention only of supporting evidentiary data for as long as is contractually necessary for client work, or for as long as is necessary for our own evidence when publishing publicly our own research in the public interest.
Communent 55 of this Code.
Topics & Methodology
 Monthly assessments of the top Russian disinformation narratives in Q1 2023 (January; February; March) From November 2022, Logically conducted a weekly evaluation of the top Russian disinformation narratives. We identified these by examining daily posts from 19 Russian state-owned or state-aligned Telegram channels, selecting the top narratives based on their reach, both in terms of frequency of appearance and dissemination across channels. Following the identification of these narratives on Telegram, we reviewed VKontakte and X for the same narratives. We determined that the cross-platform dissemination of these posts was likely for the purpose of reaching broader audiences.
 February 2023 <u>identification</u> of a French-language, cross-platform network sharing Russian disinformation focusing on anti-colonial narratives The network has engaged in influence operations in Africa since 2011, including via websites masquerading as local news. After Logically manually assessed these fake news websites, we
observed a halt in their posting in 2020, and in June 2021, a new profile called "Russosphere" emerged.

 In June 2021, the activity of these websites was replaced by a new cross-platform operation called either "Russosphere" or "En Defense de la Russie". A YouTube channel was created in November 2021, and an associated X profile went live three days before Russia's invasion of Ukraine in February 2022. Across these platforms, as well as Facebook and Telegram, "Russosphere" accounts gained more than 78,000 followers and subscribers since the first account was created. We were able to isolate the different channels across these platforms by cross-referencing usernames, bios and profile pictures. Logically was able to attribute the Russosphere accounts to Luc Michel, a self-proclaimed political activist connected to the Wagner Group, and his collaborator, Fabrice Beaur, because they were listed as administrators of the Facebook page. This investigation was conducted by creating Boolean-based keyword searches on Logically Intelligence® (LI), our flagship threat detection and platform analysis tool. These are run across historical and near real-time data from thousands of domains. Our experienced team of analysts are then able to use this data to assess the information environment.
 February 2023 assessment of how Russian narratives about Ukraine have resonated in the English language Ahead of the one-year anniversary of the Russian invasion of Ukraine, we set out to assess the context behind three major narratives promoted by Russian disinformation outlets, as well as the volume of online mentions in English-language related to said narratives. We established three research environments using LI. We utilised keyword searches related to three of the most prominent Russian narratives related to Ukraine (i.e. Nazism/Satanism/Terrorism). These keyword searches were applied across thousands of domains to identify the total volume of online mentions associated with these narratives from 1 November 2021 - 7 February 2023 to assess any changes in dissemination patterns. The data assessed includes content from social media platforms, as well as web domains, and represents both unique mentions and content shares as a function of dissemination related to the narratives. Logically accounted for potential overlap in keyword terms such as "terrorists" and "Nazis" by creating exclusions to account for any known use in relation to Russia or other actors fighting in Ukraine. In practice, this meant excluding posts referring to Russians as terrorists in the context of conversations about Ukraine. By excluding (Russia* NEAR/5 terrorist*) it was possible to remove this content and focus solely on content referring to Ukrainians as terrorists. Logically has found that the dissemination of all three narratives increased in the English language since the 2022 invasion ("Ukraine is a Nazi state" by 2,600%; "Ukraine is Satanic" by 7,300%; "Ukraine is a terrorist state" by 16,200%).
March 2023 investigation into the Russian "fact-checking" website "War on Fakes"

	 We were able to attribute the website to former Russian journalist Timofey Vasiliev by reviewing 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 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. The War on Fakes Telegram channel went live on 24 February 2022, when Russia launched its expanded invasion of Ukraine. It cited its mission as "dissecting and refuting fakes". At the time of our investigation, the most up to date details in the English language version of the website revealed Vasiliev's first name and email address, as well as a phone number, which allowed Logically to definitively attribute it to Vasiliev.
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] We are including the research mentioned in QRE 29.1.1 in this annual report we upload to the Transparency Centre for the purposes of facilitating greater awareness and availability of our 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. Outline relevant actions [suggested character limit: 2000 characters] We have circulated the information provided in QRE 29.1.1 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://www.logically.ai/investigations).

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). 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] Logically has not conducted research into the effectiveness of resilience-fostering measures on platforms - see our response to QRE 29.2.1. Reach of stakeholders or citizens informed about the project: Logically has not conducted research into the effectiveness of resilience-fostering measures on platforms - see our response to QRE 29.2.1.

VII. Empowering the fact-checking comm	nunity
--	--------

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.
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. Outline relevant actions [suggested character limit: 2000 characters]
QRE 30.2.3	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 Fact's cooperation with other fact-checkers: Logically Facts has collaborated with various other fact-checking organisations. In August 2023, the Danish fact-checking organisation, TjeKDet, asked for help in sharing information on misleading claims about the Quran burnings in the Scandinavian countries. We shared four of our fact-checks on the burning of the Quran in Sweden with them. In July 2023, Logically Facts provided local knowledge and explanations on Sweden in response to a request from Fakt Yoxla, a fact-checking organization in Azerbaijan. The request was about an MP who claimed that there are double standards against religions in Sweden, referring to how Qurans were allowed to be burnt but not the Torah. Our in-country fact-checker in Sweden provided a link to our fact-check and helped to clarify a translation that was not accurate in July 2023. Logically Facts has participated in monthly calls with European fact-checkers under the European Fact-Checking Standards Network (EFCSN) wider group to discuss challenges, initiatives and funding opportunities.

In December 2023, one of our fact-checkers was selected to be part of a team of 5 European fact-checkers joining a team of 5 Arab fact-checkers to come together in Amman, Jordan, to collaborate and work together to fact-check the COP28.
Logically Facts participated in the EU Disinfo Lab summit in Poland, the GlobalFact 10 in South Korea, and the EFCSN- EDMO conference in Belgium, among others, to connect and discuss with fact-checking organizations in Europe and around the world ideas, challenges and projects in the mis/disinformation space.
Logically Facts led two sessions in the GlobalFact 10 to address some of the main challenges and opportunities of the fact-checking community. One session was called 'Tackling misinformation at speed and scale: Empowering fact-checkers through collaboration and technology' and the aim was to facilitate a discussion about how AI-powered products could help us in our daily work at scale and in record time. The other session was called 'Perception Is Reality: Public Research on the Fact-Checking Industry'. Logically Facts surveyed over 6,000 people in India, the UK, and the US to better understand how the public in each country perceives fact-checking, mis- and disinformation, and the role technology plays as it relates to both. We led discussions in both sessions on how we can build better products to help fact-checkers in their daily work and how we can help build greater public trust in fact-checking
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 between January and December 2023, 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
	- We are a <u>verified Signatory</u> of the International Fact-Checking Network (IFCN) since 2020.

 Logically Facts has applied to the European Fact-Checking Standards Network (EFCSN). We have been involved in the development of the EFCSN since the project's inception in February 2022. We were part of the Working Committee that drafted the articles that became part of the Code. Logically Facts has been part of the EFCSN Wider Group, composed of all European fact-checking organizations, which meets regularly to discuss the development of the EFCSN e.g. as regards prospective projects, funding, issues, and training. <u>Ethics</u>
 Our internal ethics process is based on our Ethics Charter; compliance therewith is overseen by our Ethics Subcommittee which is composed of senior employees. It derives from commitments to Logically's shareholders and our Board, as well as the IFCN. We will not enter into any contract which contradicts the principles of enhancing civic discourse, protecting democratic debate and process, and providing access to trustworthy information. We will not enter into any contract where there is a reasonable likelihood that the client would use the information we find to cause undue harm to any person or group or threaten human rights. We will not engage in any partnership which would undermine our commitment to political non-partisanship. In 2023 we introduced a new due diligence mechanism whereby our Ethics Subcommittee reviews prospective clients and the intended scope of work to identify risks of prohibited clients or use cases. Effectively it creates a two-stage process whereby the logging of any new customer opportunities generates a warning that this opportunity must first be verified against our list of prohibited clients and use-cases. No new contract can pass this review without unanimous agreement that there is no conflict of interest that might undermine our ethics commitments. All our commercial contracts include a limited and targeted scope for the use of our products and services; any violation thereof will result in the termination of our services.
 Prohibited Customer Types include: Political parties and political movements; Military organisations/military personnel of: The North Atlantic Treaty Organization and its member countries, subject to the condition below; A member country of the Quadrilateral Security Dialogue; A member country of the Five Eyes Intelligence Oversight and Review Council and Switzerland, in conjunction with defensive national security use cases and in accordance with the restrictions on 'Prohibited Use Cases'. Any commercial relationship with military organizations/military personnel of Albania, Turkey, or any country or alliance not captured in the categories listed above will need to be thoroughly evaluated and approved by the Ethics Committee on a case-by-case basis. Terrorist organisations/personnel; Religious organisations/personnel; Any government client located in a country which, according to the Global State of Democracies Indices (GSDI), the Ethics Committee determines has unacceptably low levels of democracy, including without limitation any country classified by the GSDI as an "authoritarian regime" or "hybrid regime" excluding Singapore. Any non-government entity or individual located in a country which satisfies both the following conditions: It is determined by the Ethics Committee to have unacceptably low levels of democracy as per the GSDI; and

 It has a score lower than 0.50 on the World Justice Project's most recent edition of the Rule of Law Index (RLI). Any non-government entity or individual located in a country which is determined by the Ethics Committee to have unacceptably low levels of democracy as per the CSDI and which has a score of 0.50 or higher on the most recent edition of the RLI, but where the entity or individual is determined by the Ethics Committee to be 'high risk' on the basis of factors including its funding and ownership and involvement in adverse events. Any other type of customer (based on any of the foregoing characteristics or otherwise) which the Ethics Committee may determine to pose a material threat to the Ethics Statement and/or Client Ethics Policy. Prohibited Use Cases include: "Offensive" or "attack" use cases, defined as follows: Any efforts that are part of or support the use of force against a state and/or a cyber intervention that violates intermational humanitarian law, not including any actions compliant with the laws of war or that constitute self-defence. Any efforts to spread misinformation or disinformation to support or promote propaganda for a war or any other use of force. Any disproportionate response to foreign interference to any other deliberate attempt to spread disinformation against a state or non-state actor, including violations of the other conditions in this Annexure. Any disproportionate response to foreign theruge through the deployment of coordinated inauthentic behaviour. Any efforts to undermine freedom of speech and expression, including atments to restrict freedom of the press, which do not fit within reasonable restrictions provided by law and necessary for the protection of mational security. Public order and public health. Any efforts to undermine feedom of speech and expression,
sensitive information or intellectual property. - Political advertising; - Any use case which uses any part of the Company's product, data and/or insights to misrepresent the position of the
Transparency

We are rigorous in the maintenance of records about all of our processes, reviews and feedback to ensure transparency and accountability.
Independence & Non-partisanship
 As a Signatory to the IFCN and prospective member of the EFCSN, we are required to uphold commitments to non-partisanship and fairness in our fact-checking work, transparency of sources, and transparency of funding and organisation. We require our fact-checking staff to disclose any potential conflicts of interest that may arise in working on any project and also to determine in advance whether working on a project might undermine our reputation for non-partisanship. No part of the business has any commercial, institutional or financial relationships with any politician or political party. All staff are prohibited from conducting any activity which might unduly damage our reputation for non-partisanship. Our editorial team uses data and analytics to identify and prioritise claims, based on their reach, traction, influence or relevance to current affairs. Claims will only be fact-checked if they: Are made in a public forum; Can be broadly assessed as reasonable/truthful or not; Can be interpreted as an assertion of factual information; Are in the public interest, and not from any one side of a debate - in respect of our apolitical stance; Meet the appropriate standards of interest and fairness; and If it is not irresponsible to do so i.e., due to a lack of expertise or sufficient context, dissemination by trolls, or the claim is a harmful conspiracy without journalistic impetus for rebuttal.
 Editorial control Exercised by our Global Head of Fact-Checking who is responsible for editorial policy and standards in the editorial team (i.e. any potentially contentious editorial decisions, complaints or necessary corrections); Each fact-check includes a call to action, encouraging users to contact our editorial team with comments, questions, complaints, and more claims to fact-check; Logically Facts has access to the Government Affairs team for specialists in internal regulation and policy from whom our fact-checkers can obtain advice, guidance and assistance to ensure that the team's workflow and standards are consistent with the best practices and policies of the global fact-checking community.

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
	re contains all the relevant information related to the implementation of the Code's Commitments and -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]
	The administration of the Transparency Centre website has been transferred fully to the community of the Code's signatories, with VOST Europe taking the role of developer.

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	The common Transparency Center has received around 35.000 views between July 1st 2023 and December 31st 2023. The average engagement time on the website is 1m11s and reports have been downloaded more than 9.000 times.

	IX. Permanent Task-Force	
	Commitment 37	
is chaired by the European Commission, and includes re	Force. The Task-force includes the Signatories of the Code and representatives from EDMO and ERGA. It epresentatives of the European External Action Service (EEAS). The Task-force can also invite relevant 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] Attended Taskforce Plenary sessions on 5 June and 7 December 2023 In June, Logically participated in a panel discussion on generative AI and its impact on disinformation. We highlighted the risk that the democratisation of generative AI tools could exacerbate the problem of disinformation ahead of the European elections taking place in June 2024. We argued that society can remain progressive by developing this technology further for positive outcomes. We emphasised the importance of media literacy initiatives to ensure that counter-disinformation actions have a meaningful impact. In December, Logically presented a proof of concept of a multilingual, multimodal product that we are developing to facilitate AI-enabled identification of fact-check-worthy videos from a large dataset, with a view to reducing the grunt work of fact-checkers deciding which claims to verify.

X. Monitoring of Code	
	Commitment 38
The Signatories commit to dedicate adequate financial ar their commitments under the Code.	nd human resources and put in place appropriate internal processes to ensure the implementation of
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]
	Logically's operations span the US, UK and India. Our coverage can include, but does not specifically target, EU Member States.

 We have expanded on the number of team members co-authoring this report and overseeing Logically's overall compliance with the Code since the publication of our 2023 report. The designated staff with these responsibilities are: The Senior Government Affairs Manager (EU/UK), who reports to the Global Head of Government Affairs 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 Government 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 to create a new due diligence process to avoid any potential misuse of our products and services; 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 OState 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.

Reporting on the service's response during a period of crisis

Reporting on the service's response during a crisis

War of aggression by Russia on Ukraine

Threats observed or anticipated at time of reporting: [suggested character limit 2000 characters].

With regards to the war in Ukraine, Logically acknowledges a threat to the company that manifests in specific staff responsible for undertaking open-source intelligence investigations being mentioned in the discourse of malicious actors. While we do not consider the threat level to be high, it is relevant to note that specific staff are targeted in this way.

Mitigations in place at time of reporting: [suggested character limit: 2000 characters].

Logically has put in place active monitoring systems in order to identify such mentions of our open-source intelligence analysts.

[Note: Signatories are requested to provide information relevant to their particular response to the threats and challenges they observed on their service(s). They ensure that the information below provides an accurate and complete report of their relevant actions. As operational responses to crisis/election situations can vary from service to service, an absence of information should not be considered a priori a shortfall in the way a particular service has responded. Impact metrics are accurate to the best of signatories' abilities to measure them].

Integrity of Services

Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.

Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention:
	In response to the war in Ukraine, with respect to Commitments 14 and 16, Logically began paying specific attention to narratives related to the conflict, whereby the major narratives we observed through our open-source intelligence (OSINT) investigations began directing our responses. We conducted specific assessments of Telegram as well as the Russian social media platform, VKontakte, to analyse internal narratives within Russia with a view to monitoring messaging signals that may be used later in disinformation campaigns.
	We also started dedicating more of our resources to non-English content. This led to our <u>discovery</u> in February 2023 of a French-language, cross-platform network called either "Russosphere" or "En Defense de la Russie", which shared Russian disinformation focusing on anti-colonial narratives.
	 The individuals behind the network have engaged in influence operations in Africa since 2011, including via websites masquerading as local news. Logically tracked these fake news websites up to its manifestation as a new profile called "Russosphere" in June 2021. At this point, the activity of these websites was replaced by a new cross-platform operation called either "Russosphere" or "En Defense de la Russie". A YouTube channel was created in November 2021, and an associated X profile went live three days before Russia's invasion of Ukraine in February 2022. Across these platforms, as well as Facebook and Telegram, "Russosphere" accounts gained more than 78,000 followers and subscribers since the first account was created. We were able to isolate the different channels across these platforms by cross-referencing usernames, bios and profile pictures. Logically was able to attribute the Russosphere accounts to Luc Michel, a self-proclaimed political activist with reported connections to the Wagner Group, and his collaborator, Fabrice Beaur, because they were listed as administrators of the Facebook page.
	Logically had not previously engaged in the attribution of foreign nationals in our OSINT investigations; since the outbreak of the war, we have now done this twice on Russia-affiliated actors i.e. the Russosphere cross-platform network cited above, and our War on Fakes investigation:
	 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. A review of his career as far back as 2011 revealed several roles where Vasiliev was a known affiliate of groups associated with Russian propaganda e.g. the Russian propaganda outlet Ridus. 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. The War on Fakes Telegram channel went live on 24 February 2022, when Russia launched its expanded invasion of Ukraine. It cited its mission as "dissecting and refuting fakes".
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available:
	As a result of the investigation to unmask the operator of War on Fakes, the said operator was been added to sanctions lists by the EU and Switzerland. The EU Official Journal <u>entry</u> of 28 July 2023, which set out the restrictive measures in respect of actions deemed to undermine or threaten the territorial integrity, sovereignty and independence of Ukraine, specified that the reason this individual was sanctioned was because of his role in War on Fakes.

Empowering the Research Community	
Outline approaches pertinent to t	his chapter, highlighting similarities/commonalities and differences with regular enforcement.
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention:
	In response to Logically's open-source intelligence (OSINT) analysts being targeted by malicious actors through mentions in the latter's discourse, we have implemented enhanced operational security measures to ensure the safety of our analysts and the integrity of our operations.
	We have intensified our focus on collecting data in a more deliberate and structured manner, moving towards more formalised intelligence collection procedures. This includes adopting a systematic approach to data collection, utilising predefined methodologies and frameworks to ensure consistency and accuracy in our analysis.
	This shift has been particularly evident in our approach to tracking influence operations and the spread of disinformation with respect to Commitment 29, especially in light of the conflict in Ukraine. We now collect and report data in a way that is much more geared towards state-backed operations, such as those seen coming out of Russia.
	To address the evolving security challenges, we are enhancing our security protocols. This includes reviewing and updating our methods for managing attribution, and ensuring that our practices are in line with ethical codes of practice. This involves the ethical and responsible identification and attribution of sources of information, maintaining the privacy and rights of individuals and entities involved as well as ensuring the secure handling of data and communications.
	Additionally, we are implementing measures to enhance analyst safety, such as providing regular security training, conducting regular security audits, implementing secure communication channels, and employing multi-factor authentication for accessing sensitive systems.
	The implementation of multi-factor authentication for accessing sensitive systems not only helps to secure these systems but also contributes to analysts' safety. By ensuring that only authorised personnel can access sensitive systems, we reduce the risk of unauthorised access by malicious actors, thus enhancing the overall safety and security of our analysts.
	To meet the ever-changing security landscape, we are committed to continuously monitoring and updating our security practices, staying vigilant against emerging threats, and adapting our procedures accordingly.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available: N/A

Reporting on the service's response during a crisis

Israel-Hamas conflict

Threats observed or anticipated at time of reporting: [suggested character limit 2000 characters].

Mitigations in place at time of reporting: [suggested character limit: 2000 characters].

[Note: Signatories are requested to provide information relevant to their particular response to the threats and challenges they observed on their service(s). They ensure that the information below provides an accurate and complete report of their relevant actions. As operational responses to crisis/election situations can vary from service to service, an absence of information should not be considered a priori a shortfall in the way a particular service has responded. Impact metrics are accurate to the best of signatories' abilities to measure them].

Integrity of Services

Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.

Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention:
	In response to the Israel-Hamas conflict, with respect to Commitment 14, Logically began producing weekly reports on the tactics, techniques and procedures (TTPs) we were observing.
	For the first time, we began analysing state-level TTPs based on the assessment of five separate groups of influencers, including from Iran, China and Russia. The expansion of our tracking to include Iranian accounts was new and in direct response to the Israel-Hamas conflict. Logically also began assessing sentiment-based influencers i.e., those whom are pro-Israel and pro-Palestine.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available: N/A

Reporting on the service's response during a crisis	
	Empowering Users
Outline approaches pertinent to t	his chapter, highlighting similarities/commonalities and differences with regular enforcement.
Specific Action applied (with	Description of intervention:
reference to the Code's relevant Commitment and Measure)	With respect to Commitment 17, Logically Facts partnered with TikTok in December 2023 on a campaign that consisted of in-app information hubs on media literacy (Swedish hub link, Finnish hub link). This was surfaced to users through the search of keywords related to media literacy topics with the hub featuring Logically Facts' educational videos (3 videos in Swedish, 3 videos in Finnish) covering topics such as lateral reading, a guide on Al-generated images and reading beyond the headlines. In light of the Israel-Hamas conflict, this campaign had a more general message so this action could relate to this conflict for an EU audience.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available:
	The three Swedish videos had over 8 million views, and the three Finnish videos had over 9 million views (data up to date as of 1 February 2024).
	Empowering the Research Community
Outline approaches pertinent to t	his chapter, highlighting similarities/commonalities and differences with regular enforcement.
Specific Action applied (with	Description of intervention:
reference to the Code's relevant Commitment and Measure)	In response to the Israel-Hamas conflict, with respect to Commitment 29, Logically made several changes to the methodologies we use to track influence operations and the spread of disinformation.
	For example, we began looking at more satellite data for the purposes of verifying the occurrence of explosions. It is worth noting that the availability of satellite data of this kind has increased since 2022 i.e. via NASA's Fire Information for Resource Management System satellite (FIRMS) that detects fire and heat.
	Logically also increased attention towards data collection in the Farsi and Arabic languages, so as to better track narratives related to the conflict.

Reporting on the service's response during a crisis	
	Lastly, given that the conflict was initiated in the context of a widespread democratisation of generative AI tools, we ensured that we held an increased awareness of AI-generated content like deepfakes in our tracking of influence operations and spread of disinformation. This included conducting dedicated trainings for staff on the detection of multimodal content.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available: N/A
	Empowering the Fact-Checking Community
Specific Action applied (with	his chapter, highlighting similarities/commonalities and differences with regular enforcement. Description of intervention:
reference to the Code's relevant Commitment and Measure)	As part of the International Fact-Checking Network and the European Fact-Checking Standards Network wider group, we have responded to requests from other fact-checking organisations as regards our coverage of the Israel-Hamas conflict. We have shared our fact-checks and analyses on 'Pallywood' and crisis actors claims. We also offered our help and support for collaboration wherever needed, with respect to our obligations under Commitment 30.
	As result, in December 2023, Logically Facts initiated a collaboration with the Jordan-based fact-checking organisation Fatabyyano to help us translate videos and text related to the Israel-Hamas conflict from Arabic into English. Fatabyyano also flags misleading claims that are going viral about the Israel-Hamas conflict for our team to assess if we can fact-check them.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available: N/A

Reporting on the service's response during an election

Reporting on the service's response during an election		
	European Elections 2024	
Threats observed or anticipated a	at time of reporting: [suggested character limit 2000 characters].	
Mitigations in place – or planned	- at time of reporting: [suggested character limit: 2000 characters].	
[Note: Signatories are requested to provide information relevant to their particular response to the threats and challenges they observed on their service(s). They ensure that the information below provides an accurate and complete report of their relevant actions. As operational responses to crisis/election situations can vary from service to service, an absence of information should not be considered a priori a shortfall in the way a particular service has responded. Impact metrics are accurate to the best of signatories' abilities to measure them].		
	Integrity of Services	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.		
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention: Ahead of the European elections due to take place 6-9 June 2024, Logically plans to produce dedicated reporting both ahead of and after these democratic processes with a view to achieving a greater focus on pre-emptive awareness. We believe this will contribute to Commitment 14 as regards the identification of tactics, techniques and procedures employed by disinformation actors during this particular electoral process.	

	Indication of impact (at beginning of action: expected impact) including relevant metrics when available: N/A
	Empowering Users
Outline approaches pertinent to t	his chapter, highlighting similarities/commonalities and differences with regular enforcement.
Specific Action applied (with	Description of intervention:
reference to the Code's relevant Commitment and Measure)	In November 2023, Logically Facts' Head of Editorial Operations in Europe, and Logically's Senior Manager of Goverment Affairs, attended the conference entitled 'Fact-checking and beyond: Building resilience for the 2024 European Elections' which was organised by the European Parliament, European Digital Media Observatory and European Fact-Checking Standards Network. After the conference, Logically Facts organised online meetings with EU press officers in the European countries where the company is currently present (Ireland, Sweden, Denmark and Finland) to identify areas of collaboration, information-sharing and coverage plans ahead of the European elections.
	Logically Facts has defined a plan for Q1 and Q2 2024 to cover the European elections. This involves identifying accounts spreading misinformation across social media platforms, creating dashboards to monitor online misinformation, identifying emerging narratives and claims, and creating media literacy interventions and prebunks around important topics related to the European elections, in line with Commitment 17.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available:
	For 2023, the aim was to increase awareness within the European institutions about Logically Facts' work, and to explore opportunities for collaboration. We connected with EU press officers in 4 European countries with whom we have now direct communication channels.
	Empowering the Research Community
Outline approaches pertinent to t	his chapter, highlighting similarities/commonalities and differences with regular enforcement.
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention: Ahead of the European elections due to take place 6-9 June 2024, Logically is taking lessons learned from the impact of AI-generated deepfakes on recent electoral processes in countries like Slovakia. Therefore, we will be paying close attention to deepfakes when tracking influence operations and the spread of disinformation as per Commitment 29.

	Indication of impact (at beginning of action: expected impact) including relevant metrics when available: N/A
	Empowering the Fact-Checking Community
Outline approaches pertinent to t	his chapter, highlighting similarities/commonalities and differences with regular enforcement.
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	 Description of intervention: With respect to Commitment 30, Logically Facts has been part of the European Fact-Checking Standards Network (EFCSN) wider group to discuss how the different fact-checking organisations could contribute to fighting misinformation during the European Parliament elections. Logically Facts will be part of two different EFCSN collaborations in 2024: European Climate Foundation: Logically Facts will participate in the Climate Facts project alongside other European fact-checking organisations with a view to increasing cross-country collaboration in detecting and debunking climate disinformation while promoting access to verified climate information. Elections24Check: Logically Facts with other European fact-checking organizations under the EFCSN umbrella will participate in a project in cooperation with Google to combat disinformation around the EU elections. One of the tasks will be to contribute to a database in which all EFCSN members ingest their fact-checks surrounding the European elections.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available: N/A