

Code of Practice on Disinformation –
Report of Microsoft for the period
1 July – 31 December 2024

Table of Contents

Executive Summary	5
Subscription per Service overview during the Reporting Period	10
II. Scrutiny of Ad Placements.....	15
Commitment 1	16
Commitment 2	28
Commitment 3	38
III. Political Advertising	41
Commitment 4	42
Commitment 5	44
Commitment 6	46
Commitment 7	46
Commitment 8	49
Commitment 9	49
Commitment 10.....	49
Commitment 11.....	50
Commitment 12.....	50
Commitment 13.....	50
IV. Integrity of Services	51
Commitment 14.....	52
Commitment 15.....	83

Commitment 16.....	88
V. Empowering Users	92
Commitment 17.....	93
Commitment 18.....	102
Commitment 19.....	112
Commitment 20.....	117
Commitment 21.....	120
Commitment 22.....	127
Commitment 23.....	137
Commitment 24.....	140
Commitment 25.....	144
VI. Empowering the research community.....	145
Commitment 26.....	146
Commitment 27.....	153
Commitment 28.....	156
Commitment 29.....	159
VII. Empowering the fact-checking community.....	160
Commitment 30.....	161
Commitment 31.....	165
Commitment 32.....	170
Commitment 33.....	171
VIII. Transparency Centre	173
Commitment 34.....	174
Commitment 35.....	175
Commitment 36.....	176

IX. Permanent Task-Force	178
Commitment 37.....	179
X. Monitoring of Code	181
Commitment 38.....	182
Commitment 39.....	183
Commitment 40.....	183
Commitment 41.....	185
Commitment 42.....	186
Commitment 43.....	187
Commitment 44.....	188
Reporting on the services' response during a period of crisis.....	189
War of aggression by Russia on Ukraine	190
Israel-Hamas Conflict	200
Reporting on the services' response during an election.....	208
2024 French Parliamentary Elections.....	209
2024 Romanian Presidential Elections	223

Executive Summary

Microsoft welcomes the opportunity to file this fifth report on our compliance with the commitments of the strengthened 2022 EU Code of Practice on Disinformation, covering the second half of 2024. At Microsoft, we are committed to instilling trust and security across our products and services, and across the broader web. We recognise that information integrity is a key element in empowering users to access the information they need and freely express themselves. We also recognize that there is not a one size fits all approach to this work, and instead there needs to be a whole of society strategy that recognizes that not all services or platforms are the same and that there are a variety of efforts that can be effective in improving the information environment and empowering the public.

One opportunity is to continue employing AI as a resource in assisting and streamlining important work in detecting and assessing cyber enabled foreign influence operations. The harmful use of AI can also pose challenges in the information integrity space, including improved efficiency of deceptive and malicious images and videos, as malicious threat actors continue to build their capacity to create highly deceptive content efficiently. This requires continuous improvement and response to changing tactics. Microsoft's services are fully committed to utilising best in class tools and technology to help mitigate the risks of its services being misused.

Microsoft is taking a cross-product, whole-of-company approach to ensure the responsible implementation of AI. This starts with our [Responsible AI Principles](#). Building on those principles in June of 2022, Microsoft released our [Responsible AI Standard v.2](#) and [Information Integrity Principles](#) to help set baseline standards and guidance across product teams. Recognizing that there is an important role for government, academia and civil society to play in the responsible deployment of AI, we also created a [roadmap for the governance of AI](#) across the world as well as creating a vision for the responsible advancement of AI, both inside Microsoft and throughout the world, [including specifically in Europe](#). For more information on Microsoft's commitment to Responsible AI and ongoing internal and external efforts, we encourage you to review our [Responsible AI hub](#), which offers a range of information, tools, and resources related to the ethical and responsible use of AI technologies. It includes detailed information about Microsoft's internal Responsible AI processes and tools which can be used to responsibly develop and deploy AI products, including our first annual [Responsible AI Transparency Report](#). In addition, Microsoft recently released a [white paper](#) focused on policy steps that can be taken to reduce the harms of abusive AI-generated content.

Serving as a leader in AI research, we are committed to proactively publicize our threat detection efforts for the benefit of the AI community, regulators, and broader society. [As such, we have adopted six focus areas to combat the harmful use of deceptive AI:](#)

1. A strong safety architecture
2. Durable media provenance and watermarking
3. Safeguarding our services from abusive content and conduct
4. Robust collaboration across industry and with governments and civil society
5. Modernized legislation to protect people from the abuse of technology
6. Public awareness and education

Additionally, we will continue to build upon these approaches to Responsible AI. For example, recognizing both the enormous potential for generative and other forms of AI to transform the world of work in positive ways and the potential risks AI presents in that context, LinkedIn published its framework of [Responsible AI Principles](#), which is inspired by and aligned with Microsoft's Responsible AI Principles. LinkedIn provides more details on these principles in our response to Commitment 15.

Since our last report, Microsoft has continued to work with EU Member States and EU institutions to protect elections from cyber enabled influence operations by malicious threat actors. As part of that work, Microsoft and LinkedIn, along with 25 other companies, continued efforts to meet the commitments of the [Tech Accord to Combat Deceptive Use of AI in 2024 Elections \(Tech Accord\)](#). We believe the success of the Tech Accord and our work together have contributed to the limited impact of deceptive AI-generated election content throughout the elections across the European Union in 2024.

Meeting the Tech Accord's commitments made it more difficult for malicious threat actors to use legitimate tools to create deceptive AI-generated election content, while simultaneously simplifying the process for users to identify authentic content. To meet its Tech Accord commitments, Microsoft moved forward with several important initiatives that are detailed further in this report. For example:

- Microsoft is harnessing the data science and technical capabilities of our AI for Good Lab and Microsoft Threat Analysis Center (MTAC) teams to better assess whether abusive content—including that created and disseminated by malicious threat actors—is synthetic or not. Microsoft AI for Good has been improving our detection model (image, video) to assess whether media was generated by AI. The model is trained on approximately 200,000 examples of AI and real content. AI for Good continues to invest in creating sample datasets representing the latest generative AI technology. When appropriate, the team calls on the expertise of Microsoft's Digital Crimes Unit to invest in and operationalize the early detection of AI-powered criminal activity and respond fittingly, through the filing of affirmative civil actions to disrupt and deter that activity and through threat intelligence programs and data sharing with customers and government.
- As part of our commitments related to public awareness and engagement, Microsoft ran a campaign titled [Check. Recheck. Vote.](#) containing a series of public messages and stood up an AI and Elections [website](#) focused on engaging voters about the risks of deceptive AI and where to find authoritative election information. This campaign ran across the EU, UK, and the US in the lead up to major elections. Globally, the campaign reached hundreds of millions of people, with millions interacting with the content, connecting them with official election information.
- We developed a dedicated web portal – [Microsoft-2024 Elections](#) – political candidates and election authorities can report to us a concern about a deepfake of themselves or the election process that would violate our policy on deceptive AI-generated content.
- In advance of elections across the EU, we kicked off a global effort to engage campaigns and elections authorities to deepen understanding of the possible risks of deceptive AI in elections and empower those campaigns and election officials to speak directly to their voters about these steps they can take to build resilience and increase confidence in the election. In 2024, we delivered nearly 200 training sessions for political stakeholders in 25 countries, reaching over 4300 participants. This includes almost fifty separate training events with over 500 participants across EEA, including in France prior to the parliamentary elections.

Microsoft is committed to advancing information integrity and believes that including content credentials is an important driver for this. We were a founding member of the [Coalition for Content Provenance and Authenticity](#) (C2PA). To achieve transparency, support information integrity, and empower our users, we are leveraging C2PA's "[content credentials](#)" open standard across several products. For example, since 15 May 2024, content containing the "Content Integrity" technology has been automatically labelled on LinkedIn, with users beginning to see the "Cr" icon on images and videos that contain C2PA metadata.

During the reporting period, Microsoft continued piloting Content Integrity Tools, which allowed users to add content credentials to their own authentic content. Designed as a pilot program primarily to support the 2024 election cycle and gather feedback about Content Credentials-enabled tools, during the reporting period of this report, the tools were available to political campaigns in the EU, as well as to elections authorities and select news media organizations in the EU and globally. These tools included a partnership and collaboration with fellow Tech Accord signatory, TruePic. [Announced](#) in April 2024, this collaboration leveraged TruePic's mobile camera SDK enabling campaign, election, and media participants to capture authentic images, videos and audio directly from a vetted and secure device. Called the "Content Integrity Capture App" (an app that makes it easy to directly capture images with C2PA enabled signing) launched for both Android and Apple and can be used by participants in the Content Integrity Tools pilot program.

Beyond our commitment to combat deceptive use of AI during the electoral process, we implemented additional actions safeguarding candidates, election campaigns, election authorities, and voters:

- Microsoft's Campaign Success Team supported political parties and campaigns around the world to navigate the world of AI, combat the spread of cyber influence campaigns, and protect the authenticity of their own content and images.
- Microsoft's Election Communications Hub continued to support democratic governments around the world as they build secure and resilient election processes.
- Microsoft established a Virtual Situation Room, bringing together resources across the company to monitor, support, and protect elections in France and UK.
- Bing Search implemented a multifaceted approach to election integrity and integrated specialised answers and information panels for the elections across the European Union, with a link to official sources of information, which included voting information relevant to each EU Member State.

Microsoft continued its work with other trusted third-parties as part of a larger effort to empower Microsoft users to access the trusted information they are seeking. Microsoft also announced \$2M in societal resilience grants with OpenAI and several organizations benefited from the grants during this reporting period. Additionally, WITNESS, received a grant to improve journalists' ability to counter AI threats to elections. Training sessions were conducted ahead of the 2024 elections in Ghana, Georgia, and Venezuela, reaching 250 global participants. Microsoft's collaboration with WITNESS also includes co-leading the Deepfakes Rapid Response Force.

- Microsoft continues to provide pro-bono advertising space across Microsoft surfaces to disseminate media literacy campaigns, averaging 50 million impressions per month. Beginning in March 2024 and continuing through Fall 2024, Microsoft launched a new "Be Informed, Not Misled" campaign from the News Literacy Project. Microsoft also continues their partnership with the Trust Project, boosting their campaign to build audience literacy on evaluating the credibility of the content they encounter.
- In May 2024, Microsoft, in collaboration with OpenAI, launched the Societal Resilience Grants to support various organizations in promoting AI literacy, ethical AI use, and societal resilience against AI-related challenges. The grants were awarded to the Older Adults Technology Services from AARP, International IDEA, Partnership on AI, Coalition for Content Provenance and Authenticity (C2PA), and WITNESS. These initiatives have reached national election bodies in 26 countries, 500,000 older adults, and 250 global journalists, demonstrating a comprehensive approach to addressing AI threats and fostering responsible AI practices.

These initiatives underscore Microsoft's commitment to fostering a resilient and informed society in the age of AI. These grants build on an existing effort by Microsoft to support media, AI, and information literacy globally. We have continued our work with leading news and media literacy nonprofits, including the News Literacy Project (NLP), a collaboration led by The Trust Project on the Trust Indicators, and Verified, to develop campaigns built on industry research and best practices. Microsoft provided funding for the research and development of public awareness and education campaigns and supported partners with threat intelligence insights, technical expertise, and increased visibility

through in-kind ad space on Microsoft platforms. Microsoft also worked to reach young learners with dynamic and entertaining content that builds knowledge and skills. For instance,

Microsoft has subscribed to the Code of Practice with the following services:

- Bing Search is an online search engine with the primary objective of connecting users to the most relevant search results from the web. Users come to Bing with a specific research topic in mind and expect Bing to provide links to the most relevant and authoritative third-party websites on the Internet that are responsive to their search terms. Therefore, addressing misinformation or disinformation in organic search results often requires a different approach than may be appropriate for other types of online services, as over-moderation of content in search could have a significant negative impact on the right to access information, freedom of expression, and media plurality. Therefore, Bing must carefully balance these fundamental rights and interests as it works to ensure that its algorithms return the most high-quality content available that is relevant to the user's queries, working to avoid causing harm to users without unduly limiting their ability to access answers to the questions they seek. In some cases, different features may require different interventions based on functionality and user expectations. While Bing's remediation efforts may on occasion involve removal of content from search results (where legal or policy considerations warrant removal), in many cases, Bing has found that actions such as targeted ranking interventions, or additional digital literacy features such as Answers pointing to high authority sources and content provenance indicators, are more effective. Bing regularly reviews the efficacy of its measures to identify additional areas for improvement and works with internal and external subject matter experts in key policy areas to identify new threat vectors or improved mechanisms to help prevent users from being unexpectedly exposed to harmful content in search results that they did not expressly seek to find. During the Reporting Period, the nature of Bing generative AI experiences evolved. In October 2024, Microsoft launched a separate, standalone consumer service known as Microsoft Copilot at copilot.microsoft.com, which offers conversational experiences powered by generative AI, and the Copilot in Bing (formerly known as Bing Chat) generative AI experience was phased out. Bing continues to offer generative AI experiences, such as Bing Image Creator and Bing Generative Search, which was launched this Reporting Period. Bing Generative Search utilizes AI to deliver a unique experience by not only optimizing search results but presenting information in a user-friendly, cohesive layout. Results also include citations and links that enable users to explore further and evaluate websites for themselves. For both of these AI-powered experiences, Bing has partnered closely with Microsoft's Responsible AI team to proactively address AI-related risks and continues to evolve these features based on user and external stakeholder feedback.
- LinkedIn is a real identity online social networking service for professionals to connect and interact with other professionals, grow their professional network and brand, and seek career development opportunities. LinkedIn is part of its members' professional identity and has a specific purpose. Activity on the platform and content members share can be seen by current and future employers, colleagues, potential business partners and recruitment firms, among others. Given this audience, members by and large tend to limit their activity to professional areas of interest and expect the content they see to be professional in nature. LinkedIn is committed to keeping its platform safe, trusted, and professional and respects the laws that apply to its services. On joining LinkedIn, members agree to abide by LinkedIn's [User Agreement](#) and its [Professional Community Policies](#), which expressly forbid members from posting information that is false or misleading.
- Microsoft Advertising is our proprietary advertising platform, which serves the vast majority of ads displayed on Bing Search and provides advertising to most other Microsoft services that display ads, as well as many third-party services. Microsoft Advertising works both with advertisers, who provide it with advertising content, and publishers, such as Bing Search, who display these advertisements on their services. Microsoft Advertising employs a distinct set of policies and enforcement measures

with respect to each of these two categories of business partners to prevent the spread of disinformation, including through discouraging and reducing the dissemination and monetization of disinformation through advertising.

As a company, we continued our efforts during the reporting period to empower users to better understand the information they consume across our platforms and products. For example, Bing compiled a specialized dataset of European Parliament election related queries in different EU languages for use by the research community and to support transparency; researchers can apply using the form found [here](#). Over the course of the next reporting period, we will continue to make this information transparent and public. Specifically, we will continue to focus on the following areas:

- Further de-funding the mechanisms malicious threat actors are using to push their narratives and propaganda and regularly evaluating and improving user and advertiser policies as needed.
- Ensuring Microsoft and LinkedIn AI products are developed consistent with Microsoft's Responsible AI Standards and LinkedIn's Responsible AI Principles, as relevant, and that risks associated with AI systems are mitigated to provide safe, trustworthy, and ethical experiences for users and, further, ensuring that our information integrity principles are integrated into AI systems included in Microsoft products.
- Continuing to monitor foreign information influence operations and actioning such intelligence appropriately through defensive search and other techniques. This includes working with trusted third parties Microsoft uses to inform its work detecting and disrupting these influence operations. This also includes adding trusted third parties in additional languages, ensuring global coverage for our information integrity work.
- Strengthening our efforts and expanding our funding in the areas of media literacy and critical thinking, aiming to include vulnerable groups and having greater language access. As part of our focus areas and commitments under the Tech Accord we will increase our partnerships to increase AI literacy efforts and build greater understanding of provenance and other trustworthiness indicators.
- Supporting good faith research into disinformation and broader disinformation trends and tactics.
- Continue to share learnings pertaining to generative AI and Responsible AI practices as products and services evolve and new threats emerge. In addition, Microsoft will continue to regularly evaluate, implement, and share best practices for addressing disinformation trends as we navigate the technological changes posed by the malicious use of AI.
- Develop new partnerships to support EU-specific risks and continue to explore further ways to help users evaluate content on our services.
- Enhance existing research tooling to provide enhanced data reporting and continue to deliver relevant data and research to support research into the spread of disinformation.
- Educating users on generative AI features, including their risks and limitations, and providing the broader public and research community with information on our approach to Responsible AI
- Implementing and regularly evaluating measures to support safe and democratic elections in the EU and to direct users to high authority sources of information about elections.

Unless stated otherwise, data provided under this report covers a reporting period of 1 July 2024 to 31 December 2024 ("Reporting Period").

Subscription per Service overview during the Reporting Period

Commitments	Measures	LinkedIn	Microsoft Advertising	Bing Search	Microsoft Corporation
II. Scrutiny of Ad Placements					
1	Measure 1.1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 1.2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 1.3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 1.4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 1.5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 1.6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	Measure 2.1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 2.2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 2.3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 2.4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	Measure 3.1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 3.2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 3.3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
III. Political Advertising					
4	Measure 4.1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 4.2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	Measure 5.1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	Measure 6.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 6.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 6.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 6.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 6.5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	Measure 7.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 7.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	Measure 7.3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 7.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	Measure 8.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 8.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	Measure 9.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 9.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	Measure 10.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 10.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	Measure 11.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 11.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 11.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 11.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	Measure 12.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 12.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 12.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	Measure 13.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 13.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 13.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IV. Integrity of Services					
14	Measure 14.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 14.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 14.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
15	Measure 15.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 15.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
16	Measure 16.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 16.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
V. Empowering Users					
17	Measure 17.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 17.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 17.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

18	Measure 18.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 18.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 18.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
19	Measure 19.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 19.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
20	Measure 20.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 20.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
21	Measure 21.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 21.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 21.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
22	Measure 22.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 22.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 22.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 22.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 22.5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 22.6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 22.7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
23	Measure 23.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 23.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
24	Measure 24.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
25	Measure 25.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 25.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VI. Empowering the Research Community					
26	Measure 26.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 26.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 26.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
27	Measure 27.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 27.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 27.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 27.4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

28	Measure 28.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 28.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 28.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 28.4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
29	Measure 29.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 29.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 29.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VII. Empowering the Fact-checking Community					
30	Measure 30.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 30.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 30.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 30.4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
31	Measure 31.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 31.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 31.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 31.4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
32	Measure 32.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Measure 32.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Measure 32.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
33	Measure 33.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VIII. Transparency Centre					
34	Measure 34.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 34.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 34.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 34.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 34.5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
35	Measure 35.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 35.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 35.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 35.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

	Measure 35.5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 35.6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
36	Measure 36.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 36.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 36.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IX. Permanent Task-Force					
37	Measure 37.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 37.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 37.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 37.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 37.5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 37.6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
X. Monitoring of the Code					
38	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
39	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
40	Measure 40.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 40.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 40.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 40.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 40.5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 40.6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
41	Measure 41.1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 41.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Measure 41.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
42	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
43	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
44	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

II. Scrutiny of Ad Placements

Commitments 1 - 3

II. Scrutiny of Ad Placements

Commitment 1

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

	C.1	M 1.1	M 1.2	M 1.3	M 1.4	M 1.5	M 1.6
We signed up to the following measures of this commitment:	LinkedIn Microsoft Advertising	LinkedIn Microsoft Advertising	LinkedIn Microsoft Advertising	LinkedIn Microsoft Advertising	LinkedIn	LinkedIn Microsoft Advertising	LinkedIn Microsoft Advertising

	LinkedIn	Microsoft Advertising
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	No
If yes, list these implementation measures here [short bullet points].	New Implementation Measures Not applicable.	New Implementation Measures Not applicable.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures LinkedIn plans to continue to assess its policies and services and to update them as warranted.	Planned Implementation Measures Microsoft Advertising plans to continue to assess its policies, services and accreditations to update them as warranted.

Measure 1.1	LinkedIn	Microsoft Advertising
QRE 1.1.1	<p>LinkedIn prohibits misinformation and disinformation on its platform, whether in the form of organic content or in the form of advertising content. LinkedIn's Professional Community Policies, which apply to all content on LinkedIn's platform, expressly prohibit false and misleading content, including misinformation and disinformation:</p> <ul style="list-style-type: none"> • Do not share false or misleading content. Do not share content that is false, misleading, or intended to deceive. Do not share content to interfere with or improperly influence an election or civic process. Do not share content that directly contradicts guidance from leading global health organisations and public health authorities; including false information about the safety or efficacy of vaccines or medical treatments. Do not share content or endorse someone or something in exchange for personal benefit (including personal or family relationships, monetary payment, free products or services, or other value), unless you have included a clear and conspicuous notice of the personal benefit you receive and have otherwise complied with our Advertising Policies. <p>LinkedIn provides specific examples of false and misleading content that violates its policy via a Help Center article on False or Misleading Content.</p> <p>LinkedIn's Advertising Policies incorporate the Professional Community Policies provision, and similarly prohibit misinformation and disinformation. In addition, LinkedIn's Advertising Policies also prohibit fraudulent and deceptive ads, and require that claims in an ad have factual support:</p>	<p>Microsoft Advertising prohibits misinformation and disinformation on its network.</p> <p>As reported in QRE 1.2.1, Microsoft Advertising works with selected, trustworthy publishing partners and requires these partners to abide by strict brand safety-oriented policies to avoid providing revenue streams to websites engaging in misleading, deceptive, harmful, or insensitive behaviours.</p> <p>Additionally, Microsoft Advertising has network-wide policies to avoid the publishing and carriage of harmful Disinformation and the placement of advertising next to Disinformation content. Such policies prohibit ads or sites that contain or lead to Disinformation. To enforce this policy, "We may use a combination of internal signals and trusted third-party data or information sources to reject, block, or take down ads or sites that contain disinformation or send traffic to pages containing disinformation. We may block at the domain level landing pages or sites that violate this policy." Please see here for our main policy page.</p>

	<ul style="list-style-type: none"> ○ Fraud and Deception: Ads must not be fraudulent or deceptive. Your product or service must accurately match the content of your ad. Any claims in your ad must have factual support. Do not make deceptive or inaccurate claims about competitive products or services. Do not imply you or your product are affiliated with or endorsed by others without their permission. Additionally, make sure to disclose any pertinent partnerships when sharing advertising content on LinkedIn. Do not advertise prices or offers that are inaccurate - any advertised discount, offer or price must be easily discoverable from the link in your ad. <p>Of note, unlike some other platforms, LinkedIn does not allow members to monetise or run ads against their content, nor does it offer a member ad revenue share program. Thus, members publishing disinformation on LinkedIn are not able to monetise that disinformation or collect advertising revenue via LinkedIn. LinkedIn has instead reported the number of ads it restricted on its platform during the period.</p>	
SLI 1.1.1 – Numbers by actions enforcing policies above (specify if at page and/or domain level)	<p>Methodology of data measurement:</p> <p>The table below reports metrics concerning ads LinkedIn restricted under the misinformation policies in QRE 1.1.1.</p> <p>The metrics include:</p> <ol style="list-style-type: none"> 1. the number of ads LinkedIn restricted under the misinformation policies in QRE 1.1.1 between 1 July – 31 December 2024, broken out by EEA Member State; 2. the number of impressions those ads received before they were restricted. The metrics are assigned to EEA Member State based on the primary country targeting of the ad. 	<p>Methodology of data measurement:</p> <p>Microsoft Advertising assesses the impact of its actions by reporting on the individual ads that we prevented from monetizing on web properties participating in the Microsoft Advertising network (i.e., “publisher sites” that use the Microsoft Advertising services to display ads on their properties), and the number web domains that we blocked from participating in our ad network. We focus our reporting on the number of instances where ads would have been served but have been restricted from serving, thus eliminating an “impression”. Below we define this methodology as a count of Page Views.</p> <ul style="list-style-type: none"> - “Page Views” represents the number of pages viewed in which we prevented an ad from being served. This means that we proactively blocked ads before

	<p>No ads were restricted under the misinformation policies in QRE 1.1.1 between 1 July - 31 December 2024.</p> <p>The following factors may contribute to the number of ads reported by LinkedIn being lower than other platforms:</p> <ul style="list-style-type: none"> - LinkedIn is primarily a business-to-business advertising platform – that is, businesses marketing their products and services to other businesses and members in a professional capacity. - Related, because of the business-to-business nature of LinkedIn’s advertising platform, ads on LinkedIn may cost more than ads in other settings, impacting the ads run on LinkedIn. 		<p>they may be shown to a consumer. Please see SLI 1.1.2 for the Euro value of ads demonetized associated with this Page Views data.</p> <ul style="list-style-type: none"> - “Domain” represents the number of web domains which received at least one page view in a Member State. Since Microsoft Advertising blocks domains across all regions (meaning, we don’t break down the blocks at the individual country level because we apply the same globally), we are reporting on the overall number across all Member States for the current reporting period. 	
	The number of ads LinkedIn restricted under its misinformation policies in QRE 2.1.1 between 1 July – 31 December 2024	The number of impressions the ads received before they were restricted.	Page Views	Domain
Level	Ads	Impressions	Page Views	Domain
Member States				
Austria	0	0	460,850	
Belgium	0	0	0	
Bulgaria	0	0	3,504	
Croatia	0	0	5,079	
Cyprus	0	0	3,950	
Czech Republic	0	0	75,076	
Denmark	0	0	95,138	
Estonia	0	0	1,438	
Finland	0	0	0	
France	0	0	1,784,624	
Germany	0	0	4,418,339	
Greece	0	0	0	
Hungary	0	0	11,815	
Ireland	0	0	326,844	
Italy	0	0	8,256,291	

Latvia	0	0	468	
Lithuania	0	0	1,386	
Luxembourg	0	0	0	
Malta	0	0	3,032	
Netherlands	0	0	0	
Poland	0	0	23,777	
Portugal	0	0	0	
Romania	0	0	20,952	
Slovakia	0	0	0	
Slovenia	0	0	0	
Spain	1	0	0	
Sweden	0	0	0	
Iceland	0	0	0	
Liechtenstein	0	0	0	
Norway	0	0	96,441	
Total EU	0	0	15,492,563	158
Total EEA	0	0	15,589,004	158

This additional Service Level Indicator provides an estimated financial value of the actions taken by Signatories to demonetise disinformation sources (under SLI 1.1.1). It is based on media metrics available to Signatories (query/bid ¹ or impression ²) and applying an agreed-upon conversion factor provided by a third party designated by the Task-force of the Code (Ebiquity Plc.).		
SLI 1.1.2 - Preventing the flow of legitimate advertising investment to sites or content that are designated as disinformation	<p>Methodology of data measurement:</p> <p>Following the methodology developed by the Task-force Subgroup on Ad Scrutiny, this SLI considers the impressions to ads or sources that were blocked and applies an agreed-upon conversion factor to those impressions.</p>	<p>Methodology of data measurement:</p> <p>Following the methodology developed by the Task-force Subgroup on Ad Scrutiny, this SLI considers Page Views and applies an agreed-upon conversion factor to those impressions.</p>

¹ Request placed between a seller and buyer of advertising that can detail amongst other things website, specific content, targeting data inclusive of audience or content.

² Comprehensive calculation of the number of people who have been reached by a piece of media content by passive exposure (viewing a piece of content) or active engagement (visiting a destination).

	<p>As reported above, LinkedIn restricted 0 ads between 1 July – 31 December 2024 under its misinformation policies in QRE 1.1.1.</p> <p>We calculated the approximate financial value in the table by using a “blended CPM” value and the following equation:</p> <p>(Impressions/1000) x Blended CPM; where CPM means “Cost Per Mille.”</p>	<p>It should be noted, however, that Microsoft Advertising is a “pay per click” (PPC) ad network. This means that advertisers are charged following a click on the ad, and not based on the number of impressions served. We therefore calculated the approximate financial value in the table by using the “blended CPM” value provided by Ebiquity Plc. and the following equation:</p> <p>(Page Views/1000) x Blended CPM; where CPM means “Cost Per Mille.”</p> <p>As described above, Microsoft Advertising prevents serving any ads on web domains that spread disinformation. Such proactive measures block all ad traffic upfront (i.e., we act at the earliest point of identification, which could mean prior to an impression being served), which brings the monetization on those web properties down to zero. Please see SLI 1.1.1 for the associated number of advertisements that we proactively prevented from showing to a consumer.</p>
	Euro value of ads demonetised	Euro value of ads demonetised
Member States		
Austria	0	€ 1,843.40
Belgium	0	€ 0.00
Bulgaria	0	€ 5.26
Croatia	0	€ 17.78
Cyprus	0	€ 9.88
Czech Republic	0	€ 300.30
Denmark	0	€ 428.12
Estonia	0	€ 3.60
Finland	0	€ 0.00
France	0	€ 7,138.50
Germany	0	€ 19,882.53
Greece	0	€ 0.00
Hungary	0	€ 23.63

Ireland	0	€ 980.53
Italy	0	€ 28,897.02
Latvia	0	€ 1.40
Lithuania	0	€ 3.47
Luxembourg	0	€ 0.00
Malta	0	€ 9.10
Netherlands	0	€ 0.00
Poland	0	€ 35.67
Portugal	0	€ 0.00
Romania	0	€ 31.43
Slovakia	0	€ 0.00
Slovenia	0	€ 0.00
Spain	0	€ 0.00
Sweden	0	€ 0.00
Iceland	0	€ 0.00
Liechtenstein	0	-
Norway	0	€ 530.43
Total EU	0	€ 59,612
Total EEA	0	€ 60,142

Measure 1.2	LinkedIn	Microsoft Advertising
QRE 1.2.1	<p>LinkedIn does not offer a member ad revenue share program and does not allow members to monetise content they post to LinkedIn by running ads against it.</p> <p>LinkedIn displays ads in two environments: (1) on the LinkedIn platform, which accounts for the vast majority of ads; and (2) on the LinkedIn Audience Network, which allows LinkedIn advertisers to extend their reach to professionals on a curated network of approximately twenty-five thousand third-party publishers</p>	<p>Microsoft Advertising works with selected, trustworthy publishing partners and requires these partners to abide by strict brand safety-oriented policies to avoid providing revenue streams to websites engaging in misleading, deceptive, harmful, or insensitive behaviors. These publishers also benefit from the set of measures identified above that Microsoft Advertising takes with regard to advertisers, which ensures that these partners receive high-integrity, non-deceptive ads from the Microsoft Advertising platform.</p>

	<p>selected by LinkedIn (for example, Nasdaq.com, CNN.com, Vogue.com, Realtor.com).</p> <p>With respect to the first category – ads displayed on the LinkedIn platform – as noted in response to QRE 1.1.1, unlike other platforms, LinkedIn does not offer a content monetisation or an ad revenue share program to members. Thus, no member content is monetised or demonetised, and there is no ability for a member publishing disinformation to collect any advertising revenue share from LinkedIn.</p> <p>With respect to the second category – ads displayed on the LinkedIn Audience Network – LinkedIn takes a number of steps to help ensure LinkedIn advertisers' ads appear in a trusted environment and that publishers that systematically provide harmful disinformation are not included in the LinkedIn Audience Network.</p> <ul style="list-style-type: none"> ○ First, the LinkedIn Audience Network is a curated network of third-party sites and apps selected by LinkedIn. LinkedIn does not allow any blog, application, or website to join the LinkedIn Audience Network and display ads; rather, LinkedIn selects the publishers that are included in the network. ○ Second, LinkedIn has integrated with partners, such as Integral Ad Science and DoubleVerify, to help monitor the quality and brand safety of the publishers in the LinkedIn Audience Network and filter out publisher inventory that falls short of standards, such as brand safety floors. ○ Third, LinkedIn regularly reviews the publishers included in the LinkedIn Audience Network to ensure they meet LinkedIn standards and are serving LinkedIn advertisers. <p>To date, LinkedIn has periodically removed publishers from the LinkedIn Audience Network, but has not had to remove any publisher as a result of publishing disinformation.</p>	<p>Microsoft Advertising's policies with respect to these publishers include a comprehensive list of prohibited content that ads cannot serve against. Prohibited content includes, but is not limited to, Disinformation, sensitive political content (e.g., extreme, aggressive, or misleading interpretations of news, events, or individuals), unmoderated user-generated content, and unsavory content (such as content disparaging individuals or organizations). Publishers are required to maintain a list of prohibited terms and provide us with information on their content management practices where applicable. In addition to content requirements, publishers are required to abide by restrictions against engaging in business practices that are harmful to users (e.g., distributing malware).</p> <p>Microsoft Advertising reviews publisher properties and domains for policy compliance, including compliance with restrictions on prohibited content. In this review, Microsoft Advertising also considers feedback from its advertisers to help ensure a safe environment for the delivery of their advertisements and maintains a review process to investigate related advertiser complaints. Publishers are promptly notified of properties or domains that violate Microsoft Advertising's policies; such properties and domains are not approved by Microsoft for live ad traffic. If a property or domain is already live, and later found in violation of Microsoft Advertising's policies, it is removed from the network until the publisher remedies the issue.</p> <p>As stated in our revised policies, "We may use a combination of internal signals and trusted third-party data or information sources to reject, block, or take down ads or sites that contain disinformation or send traffic to pages containing disinformation."</p>
--	---	--

					Microsoft Advertising partners with third parties as sources for strategic intelligence on domains. Microsoft Advertising actions domains, based in part on these sources evaluations as foreign influence related or non-compliant.			
SLI 1.2.1	<p>Methodology of data measurement:</p> <p>As stated in response to QRE 1.2.1, LinkedIn does not allow members to monetise content they post to LinkedIn by running ads against it and has not had to remove any publisher from the LinkedIn Audience Network for publishing disinformation.</p> <p>Accordingly, the metrics for this SLI for the period 1 July – 31 December 2024 are zero.</p>				<p>Methodology of data measurement</p> <p>As reported in SLI 1.1.1, since Microsoft Advertising blocks domains globally, not at the Member State level, we are providing the global aggregate number of 158 barred for the current reporting period.</p> <p>Microsoft Advertising did not bar any accounts during the relevant reporting period. This is because we take actions by blocking web domains across the entire network, irrespective of which ad account may be promoting them.</p> <p>Microsoft Advertising did not roll out any new policies in the reporting period. Therefore, the relevant “nr. of policy reviews” is zero.</p>			
	Nr of policy reviews	Nr of update to policies	Nr of accounts barred	Nr of domains barred	Nr of policy reviews	Nr of update to policies	Nr of accounts barred	Nr of domains barred
Member States								
Global					Zero (0)	Zero (0)	Zero (0)	158
Total EU	-	-	-	-	-			
Total EEA	-	-	-	-	-			

Measure 1.3	LinkedIn	Microsoft Advertising
QRE 1.3.1	LinkedIn provides a range of information and tools to give advertisers transparency and control regarding the placement of their advertising. For example, for ads on the LinkedIn platform, LinkedIn publishes a Feed Brand Safety score for advertisers and the	Microsoft Advertising provides its customers with campaign reporting and functionalities to monitor and control ad placement across the Microsoft Advertising network. Such transparency controls are generally available via the campaign User Interface (UI) and through customer support. Transparency controls include:

	<p>public. The Feed Brand Safety score measures the number of ad impressions on the LinkedIn platform that appeared adjacent to – that is, immediately above or below within the LinkedIn feed – content removed for violating LinkedIn’s Professional Community Policies, including disinformation. From 1 July through 31 December 2024, the Feed Brand Safety score was 99%+ safe. More information about LinkedIn’s Feed Brand Safety Score is available here.</p> <p>In addition, LinkedIn publishes for advertisers and the public a semiannual transparency report, which discloses the amount of violating member content, including misinformation, that LinkedIn removed from the platform during the period. For the period from 1 January to 30 June 2024, for example, LinkedIn removed 30,497 pieces of misinformation from the platform. LinkedIn’s most recent transparency report is available here.</p> <p>For ads on the LinkedIn Audience Network, as discussed in QRE 1.2.1, LinkedIn provides tools to assist advertisers in controlling where their ads appear within the network. For example, advertisers can set up category-level blocking based on the Interactive Advertising Bureau’s (IAB) publisher category taxonomy to prevent their ads from running on certain types of publishers within the network. Similarly, advertisers can review the list of publishers within the network and create custom allow lists and block lists to ensure their ads are placed on apps and sites that meet an advertiser’s specific standards.</p>	<ul style="list-style-type: none"> - Ad delivery reports at the domain level: data reports show the website/domain where the ads are served. - Site exclusions: ability to exclude certain websites/domains from the ad campaigns to prevent ads from serving on such websites. - Negative keywords exclusions: ability to exclude certain keywords from the ad campaigns to prevent ads from serving against search queries containing such keywords. - Syndication Publisher Network Opt-Out: ability to prevent any ad delivery on the extended publisher network. In which case, all ads will serve on owned and operated properties.
Measure 1.4	LinkedIn	Microsoft Advertising
QRE 1.4.1	This Measure is not relevant or pertinent for LinkedIn as it does not buy advertising on behalf of others, inclusive of advertisers, and agencies.	This measure is not relevant or pertinent to Microsoft Advertising as it does not buy advertising, inclusive of advertisers, and agencies.

Measure 1.5	LinkedIn	Microsoft Advertising
QRE 1.5.1	As indicated in response to QRE 1.2.1, LinkedIn does not offer a content monetisation or an ad revenue share program to members. Thus, no member content is monetised or demonetised, and there is no ability for a member publishing disinformation on LinkedIn to collect advertising revenue share. As a result, LinkedIn has not undertaken independent third-party audits relative to monetisation and disinformation.	This measure is not relevant or pertinent to Microsoft Advertising, as it does not produce first party reporting. Please see QRE 1.5.2 for the relevant actions.
QRE 1.5.2	Not applicable.	<p>Microsoft Advertising undergoes yearly Media Rating Council (MRC) accreditations via third-party audit. The MRC accreditation certifies Microsoft Advertising's click measurement systems adheres to the industry standards for counting ad clicks and the processes supporting this technology are accurate. Here is the Microsoft Advertising's MRC accreditation letter. This article provides a summary of the click measurement processes and methods Microsoft Advertising employs to measure and count clicks. For additional information, please visit the IAB/MRC click measurement guidelines.</p> <p>Microsoft Advertising undergoes yearly audit by the Network Advertising Initiative (NAI) as part of the annual member's compliance review process.</p>
Measure 1.6	LinkedIn	Microsoft Advertising
QRE 1.6.1	<p>LinkedIn has integrated a number of brand safety tools and services to help advertisers understand and control the placement of their advertising and help avoid the placement of advertising next to disinformation content and/or in places or sources that repeatedly publish disinformation.</p> <p>First, it's worth noting that LinkedIn endeavours to limit the disinformation that may appear on its platform in the first place. As set out in response to QREs 17.1.1 / 18.1.3 / 18.2.1 / 23.2.1, LinkedIn has implemented automated and manual systems and processes to detect and remove content that violates our policies, including disinformation, and to take action on violative content when it's</p>	<p>As described in QRE 1.2.1, Microsoft Advertising partners with third parties as sources and references for strategic intelligence on foreign influence related or non-compliant domains. Microsoft Advertising is actioning domains based in part on information from these third parties.</p> <p>Please see QRE 1.3.1 for transparency and control functionalities.</p>

	<p>reported to us. Further, LinkedIn limits and controls the publishers that are included in the LinkedIn Audience Network, discussed in response to QRE 1.2.1.</p> <p>Second, LinkedIn has partnered with third parties, such as Integral Ad Science and DoubleVerify, to evaluate and filter advertising inventory on LinkedIn Audience Network publisher sites that falls short of standards, such as brand safety floors. These partners help evaluate and filter third-party publisher advertising inventory before a bid is placed, and decrease instances when an ad may run on an unsafe or low-quality page.</p> <p>In addition, LinkedIn has implemented a Brand Safety Hub within LinkedIn Campaign Manager. As part of the hub, advertisers can control what publisher apps and sites their ads appear on within the LinkedIn Audience Network. For example, advertisers can create custom block lists and allow lists of publisher sites within the LinkedIn Audience Network that meet an advertiser's specific standards. Similarly, advertisers can apply third-party brand safety tools to their campaigns, including DoubleVerify brand suitability profiles.</p>	
QRE 1.6.2	This QRE is not relevant or pertinent for LinkedIn as it does not buy advertising on behalf of others, inclusive of advertisers, and agencies.	This QRE is not relevant or pertinent as Microsoft Advertising does not buy advertising.
QRE 1.6.3	This QRE is not relevant or pertinent as LinkedIn is not a brand safety tool provider.	This QRE is not relevant or pertinent as Microsoft Advertising is not a brand safety tool provider.
QRE 1.6.4	This QRE is not relevant or pertinent as LinkedIn is not a ratings service.	This QRE is not relevant or pertinent as Microsoft Advertising is not a ratings service.
SLI 1.6.1	Methodology of data measurement: Not applicable.	Methodology of data measurement: N/A

II. Scrutiny of Ad Placements

Commitment 2

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

	C.2	M 2.1	M 2.2	M 2.3	M 2.4
We signed up to the following measures of this commitment:	LinkedIn Microsoft Advertising	LinkedIn Microsoft Advertising	LinkedIn Microsoft Advertising	LinkedIn Microsoft Advertising	LinkedIn Microsoft Advertising

	LinkedIn	Microsoft Advertising
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	Yes
If yes, list these implementation measures here [short bullet points].	<p>New Implementation Measures</p> <p>Not applicable.</p>	<p>New Implementation Measures</p> <p>Microsoft Advertising implemented the following measures:</p> <ul style="list-style-type: none"> - Iterated on its automated detection mechanisms <ul style="list-style-type: none"> o Improve AI model to detect clickbait and low-quality ads o Continue expanding to multiple internal domain trust signals as well as partner signals to make

		domain detection more robust
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures LinkedIn plans to continue to assess its policies and services and to update them as warranted.	Planned Implementation Measures Microsoft Advertising plans to continue to assess its policies and services and to update them as warranted.

Measure 2.1	LinkedIn	Microsoft Advertising
QRE 2.1.1	<p>As noted in response to QRE 1.1.1, LinkedIn prohibits misinformation and disinformation on its platform, whether in the form of organic content or in the form of advertising content. LinkedIn's Professional Community Policies, which apply to all content on the platform, expressly prohibit false and misleading content, including misinformation and disinformation:</p> <ul style="list-style-type: none"> - Do not share false or misleading content. Do not share content that is false, misleading, or intended to deceive. Do not share content to interfere with or improperly influence an election or other civic process. Do not share content that directly contradicts guidance from leading global health organisations and public health authorities; including false information about the safety or efficacy of vaccines or medical treatments. Do not share content or endorse someone or something in exchange for personal benefit (including personal or family relationships, monetary payment, free products or services, or other value), unless you have included a clear and conspicuous notice of the personal 	<p>As described in QRE 2.2.1, Microsoft Advertising employs a set of policies that prohibit advertising content that is misleading, deceptive, fraudulent, or harmful, including misinformation and disinformation.</p> <p>In December 2022, Microsoft Advertising rolled out revised network-wide policies to avoid the publishing and carriage of harmful Disinformation and the placement of advertising next to Disinformation content. Such policies prohibit ads or sites that contain or lead to Disinformation. To enforce this policy, "We may use a combination of internal signals and trusted third-party data or information sources to reject, block, or take down ads or sites that contain disinformation or send traffic to pages containing disinformation. We may block at the domain level landing pages or sites that violate this policy." Please see here for our main policy page.</p>

	<p>benefit you receive and have otherwise complied with our Advertising Policies.</p> <p>LinkedIn provides specific examples of false and misleading content that violates its policy via a Help Center article on False or Misleading Content.</p> <p>LinkedIn's Advertising Policies incorporate the Professional Community Policies provision, and similarly prohibit misinformation and disinformation. In addition, LinkedIn's Advertising Policies separately prohibit fraudulent and deceptive ads, and require that claims in an ad have factual support:</p> <ul style="list-style-type: none"> - Fraud and Deception: Ads must not be fraudulent or deceptive. Your product or service must accurately match the content of your ad. Any claims in your ad must have factual support. Do not make deceptive or inaccurate claims about competitive products or services. Do not imply you or your product are affiliated with or endorsed by others without their permission. Additionally, make sure to disclose any pertinent partnerships when sharing advertising content on LinkedIn. Do not advertise prices or offers that are inaccurate – any advertised discount, offer or price must be easily discoverable from the link in your ad. 	
SLI 2.1.1 – Numbers by actions enforcing policies above	<p>Methodology of data measurement:</p> <p>The table below reports the number of ads LinkedIn restricted under the misinformation policies in QRE 2.1.1 above between 1 July – 31 December 2024, broken out by EEA Member State.</p> <p>The metrics are assigned to EEA Member State based on the primary country targeting of the ad.</p>	<p>Methodology of data measurement:</p> <p>Microsoft Advertising assesses the impact of its actions by reporting on the ads that were loaded in the Microsoft Advertising campaign system but that we blocked from being displayed across our network and estimating the number of individual ad impressions that such ads would have generated (i.e., ads that would have been served to consumers).</p>

	No ads were restricted between 1 July – 31 December 2024.		“Unique Ads” are the individual advertisements (or ad creatives) loaded in the Microsoft Advertising campaign system that we blocked. During the reporting period, 2,193,970 ads were blocked globally (see “Global” total), including in all EEA Member States. For transparency purposes, the metrics mentioned in the table for each Member State are lower, as these are <i>additional</i> ads that were blocked in each respective Member State. Hence the totals for ads blocked in the EU and EEA as a whole, are in this instance larger than the Global total.			
	The following factors may contribute to the number of ads reported by LinkedIn being low: <ul style="list-style-type: none">- LinkedIn is primarily a business-to-business advertising platform<ul style="list-style-type: none">- that is, businesses marketing their products and services to other businesses and members in a professional capacity.- Because of the business-to-business nature of LinkedIn’s advertising platform, ads on LinkedIn may cost more than ads placed in other settings, impacting the ads run on LinkedIn.		“Blocked Impressions” means the individual ad impressions that such Unique Ads would have generated if not blocked. “Unique Domains” means the web domain or URLs that the Unique Ads would have directed customers to. For example, if Advertiser A loads 10 ads in the campaign system promoting two websites associated with disinformation that would have been displayed 100 times, Microsoft Advertising will report 10 Unique Ads, 100 Blocked Impressions, and two Unique Domains. In practice, however, no consumer ever see any of these ads. “Account suspension” means suspending access to the Microsoft Advertising services to advertisers who willingly or repeatedly violate our terms or policies prohibiting phishing, malware, or payment Instrument fraud. Suspended customers cannot serve ads until they redress the violation.			
	The number of ads LinkedIn restricted under the misinformation policies in QRE 2.1.1 between 1 July - 31 December 2024		The number of ads Microsoft restricted under the misinformation policies in QRE 2.1.1 between July 1, 2024 – December 31, 2024.			
			Unique Ads	Blocked Impressions	Unique Domains	Account suspension
Member States						
Austria	0		45,895	15,099,520	432	321
Belgium	0		13,602	16,341,515	489	679
Bulgaria	0		8,414	846,117	344	140
Croatia	0		5,557	589,799	254	25

Cyprus	0	6,005	385,434	285	139
Czech Republic	0	9,385	4,020,308	368	296
Denmark	0	11,955	3,736,810	377	453
Estonia	0	5,023	394,036	241	161
Finland	0	9,004	2,929,201	348	556
France	0	22,321	33,941,040	693	4378
Germany	0	184,877	169,260,210	735	7277
Greece	0	6,960	1,554,682	375	290
Hungary	0	8,412	1,381,649	336	61
Ireland	0	10,087	6,351,043	431	351
Italy	0	17,654	18,995,565	580	2022
Latvia	0	5,296	418,449	254	97
Lithuania	0	7,644	732,340	313	197
Luxembourg	0	5,616	736,362	300	43
Malta	0	4,377	274,817	241	27
Netherlands	0	13,072	13,276,757	579	1511
Poland	0	10,657	5,351,377	464	1068
Portugal	0	11,122	6,574,294	452	235
Romania	0	8,605	3,557,594	407	427
Slovakia	0	6,654	1,064,249	284	50
Slovenia	0	4,950	520,188	241	48
Spain	0	18,471	19,365,688	605	2857
Sweden	0	13,051	7,940,119	464	551
Iceland	0	3,771	312,425	222	23
Liechtenstein	0	1,058	61,850	126	5
Norway	0	13,590	3,895,944	411	426
Global		2,193,970	-	-	-
Total EU	0	2,668,636	335,639,163	10,892	24,260
Total EEA	0	2,687,055	339,909,383	11,651	24,714

Measure 2.2	LinkedIn	Microsoft Advertising
<p>QRE 2.2.1</p>	<p>LinkedIn works with numerous partners to facilitate the flow of information to tackle purveyors of disinformation, including disinformation spread by state-sponsored and institutional actors.</p> <p>LinkedIn maintains an internal Trust and Safety team composed of threat investigators and intelligence analysts to address disinformation. This team works with peers and other stakeholders, including our Artificial Intelligence modeling team, to identify and remove nation-state actors and coordinated inauthentic campaigns. LinkedIn conducts investigations into election-related influence operations and nation-state targeting including continued information sharing on threats with industry peers and Law Enforcement on a regular basis. LinkedIn works with peer companies and other stakeholders to receive and share indicators related to fake accounts created by state-sponsored actors, such as confirmed Tactics, Techniques, and Protocols (TTPs) and Indicators of Compromise (IOC). This exchange of information leads to a better understanding of the incentives of sophisticated and well-funded threat actors and how they evolve their TTPs to achieve those goals, which assists LinkedIn in their identification and removal. Any associated disinformation content is verified by our internal or external fact-checkers, and coordinated inauthentic behaviours (CIBs) are also removed by our Trust and Safety team.</p> <p>LinkedIn, along with its parent company, Microsoft, is heavily involved in threat exchanges. These threat exchanges take various forms, such as: 1) regular discussion amongst industry peers to discuss high-level trends and campaigns; and, 2) one-on-one engagement with individual peer companies to discuss TTPs and IOCs. This exchange of information leads to a better understanding of the incentives of sophisticated and well-funded threat actors and how they evolve their TTPs to achieve those goals, which assists us in their identification and removal.</p>	<p>Microsoft Advertising employs dedicated operational support and engineering resources to enforce its advertising policies detailed below, combining automated and manual enforcement methods to prevent or take down advertisements that violate its policies. Every ad loaded into the Microsoft Advertising system is subject to these enforcement methods, which leverage machine-learning techniques, automated screening, the expertise of its operations team, and dedicated user safety experts. In addition, Microsoft Advertising conducts a manual review of all advertisements flagged to its customer support team and removes advertisements that violate its policies.</p> <p>As stated in our revised policies on Disinformation, “We may use a combination of internal signals and trusted third-party data or information sources to reject, block, or take down ads or sites that contain disinformation or send traffic to pages containing disinformation.” Microsoft Advertising partners with third parties as sources for strategic intelligence on domains. Microsoft Advertising actions domains, based in part on these sources evaluations as foreign influence related or non-compliant. .</p> <p>In addition to the policy on Disinformation, Microsoft Advertising’s Misleading Content Policies prohibit advertising content that is misleading, deceptive, fraudulent, or that can be harmful to users, including advertisements that contain unsubstantiated claims, or that falsely claim or imply endorsements or affiliations with third party products, services, governmental entities, or organisations. Microsoft Advertising also has a set of Relevance and Quality Policies to manage the relevancy and quality of the advertisements that it serves through its advertising network. These policies deter advertisers from luring users onto sites using questionable or misleading tactics (e.g., by prohibiting advertisements that lead users to sites that misrepresent the origin or intent of their content).</p>

	<p>LinkedIn always stands ready to receive and investigate any leads we receive from peers and other external stakeholders. In addition to one-on-one engagement with peers, we also consume intelligence from vendors and investigate any TTPs and IOCs made available in peer disclosures. In turn, we also regularly release information about disinformation on our platform in publicly-available transparency reports and blog posts.</p>	
Measure 2.3	LinkedIn	Microsoft Advertising
QRE 2.3.1	<p>All advertising that runs on LinkedIn's platform is subject to LinkedIn's Advertising Policies. LinkedIn has implemented both automated and manual systems to help ensure that advertising on the platform complies with its Advertising Policies, and that ads that do not comply with its policies are removed.</p> <p>When an advertiser submits an advertising campaign, the campaign is evaluated by LinkedIn automated systems. If those systems determine a campaign may violate LinkedIn's policies, the campaign is rejected or forwarded to LinkedIn's advertising review team for manual review.</p> <p>The advertising review team is trained in LinkedIn's Advertising Policies and dedicated to advertising review. LinkedIn also employs a dedicated team of trainers, who not only support the onboarding of new ad reviewers, but also provide ongoing educational opportunities for reviewers.</p> <p>LinkedIn similarly employs quality assurance analysts, who provide one-on-one coaching, as well as regular monthly forums to discuss reviewers' most frequent challenges. For complex issues, reviewers have direct access to global advertising policy managers through regular office hours and dedicated escalation pathways.</p>	<p>Please see QRE 2.2.1. Microsoft Advertising blocks sites or domains that our Information Integrity expert partners deem as spreading Disinformation.</p> <p>Microsoft Advertising also rejects all ads associated with such domains and instructs its publishing partners to block ads from showing on such domains.</p>

	<p>LinkedIn members may also report ads that they believe violate LinkedIn's advertising policies, and when members report ads LinkedIn's advertising review team reviews them. To report an ad, members can click on the three-dot icon in the upper right-hand corner of every ad and select the "Hide or report this ad" option. Members are then directed to select a reporting reason, with "Misinformation" provided as a reporting option.</p>	
SLI 2.3.1	<p>Methodology of data measurement:</p> <p>The table below reports metrics concerning ads LinkedIn restricted under the misinformation policies in QRE 2.1.1. The metrics include: (1) the number of ads LinkedIn restricted under the misinformation policies in QRE 2.1.1 between 1 July - 31 December 2024, broken out by EEA Member State; (2) the number of impressions those ads received before they were restricted. The metrics are assigned to EEA Member States based on the primary country targeting of the ad.</p> <p>No ads were restricted under the misinformation policies in QRE 2.1.1 between 1 July - 31 December 2024.</p> <p>The following factors may contribute to the number of ads reported by LinkedIn being lower than other platforms:</p> <ul style="list-style-type: none"> - LinkedIn is primarily a business-to-business advertising platform -- that is, businesses marketing their products and services to other businesses and members in a professional capacity. - Because of the business-to-business nature of LinkedIn's advertising platform, ads on LinkedIn may cost more than ads on other platforms, impacting the ads run on LinkedIn. 	<p>Methodology of data measurement:</p> <p>Microsoft Advertising removed ads after the ads were shown to consumers during the relevant reporting period. Since we remove ads running in all countries, the "Nr. of ads removed" count is the same across all Member States. The low figures are due to the proactive nature of our actions, since we block most disinformation content before it is shown to consumers.</p> <p>Please see SLI 2.1.1 (Unique Ads) for the number of ads prohibited.</p>

	The number of ads LinkedIn restricted under the misinformation policies in QRE 2.1.1 between 1 July – 31 December 2024	The number of impressions the ads received before they were restricted	Nr of ads removed (as well as reach of ads before they were successfully removed)	Nr of ads prohibited (same as Unique Ads in SLI 2.1.1)
Member States				
Austria	0	0	2,527	2,239,865
Belgium	0	0	2,527	2,207,572
Bulgaria	0	0	2,527	2,202,384
Croatia	0	0	2,527	2,199,527
Cyprus	0	0	2,527	2,199,975
Czech Republic	0	0	2,527	2,203,355
Denmark	0	0	2,527	2,205,925
Estonia	0	0	2,527	2,198,993
Finland	0	0	2,527	2,202,974
France	0	0	2,527	2,216,291
Germany	0	0	2,527	2,378,847
Greece	0	0	2,527	2,200,930
Hungary	0	0	2,527	2,202,382
Ireland	0	0	2,527	2,204,057
Italy	0	0	2,527	2,211,624
Latvia	0	0	2,527	2,199,266
Lithuania	0	0	2,527	2,201,614
Luxembourg	0	0	2,527	2,199,586
Malta	0	0	2,527	2,198,347
Netherlands	0	0	2,527	2,207,042
Poland	0	0	2,527	2,204,627
Portugal	0	0	2,527	2,205,092
Romania	0	0	2,527	2,202,575
Slovakia	0	0	2,527	2,200,624
Slovenia	0	0	2,527	2,198,920

Spain	0	0	2,527	2,212,441
Sweden	0	0	2,527	2,207,021
Iceland	0	0	2,527	2,197,741
Liechtenstein	0	0	2,527	2,195,028
Norway	0	0	2,527	2,207,560
Total EU	0	0	2,527	59,711,856
Total EEA	0	0	2,527	66,312,185

Measure 2.4	LinkedIn	Microsoft Advertising
QRE 2.4.1	<p>When LinkedIn rejects or restricts an ad for violation of its policies, as described in QRE 2.3.1, LinkedIn sends the advertiser an email notification. The email notification outlines the rejection reason and advertising policy that the ad has violated.</p> <p>The notification also provides advertisers instructions regarding how they can address the violation, including by revising the ad in LinkedIn Campaign Manager to address the violations, or by contacting their sales representative or LinkedIn customer support if they require clarification or believe there has been a mistake.</p> <p>Because advertisers can address rejections a number of ways – by revising and resubmitting the advertisement, by creating a new advertisement that complies with LinkedIn’s policies, or by contacting their LinkedIn sales representative or customer support – LinkedIn does not report “appeal” and “appeal grant” metrics for ad rejections. LinkedIn has provided metrics on the number of ad restrictions as part of SLI 2.3.1 above.</p>	<p>Microsoft Advertising notifies its advertiser customers of policy violations through the following:</p> <ul style="list-style-type: none"> - Prompts in the campaign User Interface (UI) - Email notifications (for example, for account suspension) - Notifications from the assigned Account representatives, as applicable <p>Advertisers may appeal an editorial decision through the conflict-resolution process described here: How do I challenge a disapproval? (microsoft.com)</p>
SLI 2.4.1	Methodology of data measurement:	Methodology of data measurement:

	LinkedIn does not report “appeal” and “appeal grant” metrics for ad rejections as outlined in our response to QRE 2.4.1. LinkedIn has provided metrics on the number of ad restrictions as part of SLI 2.3.1 above.		Microsoft Advertising tracks appeals (at advertising creative and keyword level) in the aggregate and not at the Member State level due to the nature of its services. We are providing the aggregate global value of 4,999 total appeals during the relevant reporting period.	
	Nr of appeals	Proportion of appeals that led to a change of the initial decision	Nr of appeals	Proportion of appeals that led to a change of the initial decision
Global	N/A		4,999	3,242

II. Scrutiny of Ad Placements

Commitment 3

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

	C.3	M 3.1	M 3.2	M 3.3
We signed up to the following measures of this commitment:	LinkedIn Microsoft Advertising	LinkedIn Microsoft Advertising	LinkedIn Microsoft Advertising	LinkedIn Microsoft Advertising

	LinkedIn	Microsoft Advertising
In line with this commitment, did you deploy new implementation measures (e.g., changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	No
If yes, list these implementation measures here [short bullet points].	Not applicable	New Implementation Measures Not applicable
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No	No

If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures Not applicable	Planned Implementation Measures Not applicable
---	---	---

Measure 3.1	LinkedIn	Microsoft Advertising
QRE 3.1.1	<p>As discussed as part of QRE 2.2.1, LinkedIn works with numerous partners to facilitate the flow of information to tackle purveyors of disinformation, including disinformation spread by state-sponsored and institutional actors.</p> <p>LinkedIn maintains an internal Trust and Safety team composed of threat investigators and intelligence analysts to address disinformation. This team works with peers and other stakeholders, including our Artificial Intelligence modelling team, to identify and remove nation-state actors and coordinated inauthentic campaigns. LinkedIn conducts investigations into election-related influence operations and nation-state targeting including continued information sharing on threats with industry peers and Law Enforcement on a regular basis. LinkedIn works with peer companies and other stakeholders to receive and share indicators related to fake accounts created by state-sponsored actors, such as confirmed Tactics, Techniques, and Protocols (TTPs) and Indicators of Compromise (IOC). This exchange of information leads to a better understanding of the incentives of sophisticated and well-funded threat actors and how they evolve their TTPs to achieve those goals, which assists LinkedIn in their identification and removal. Any associated disinformation content is verified by our internal or external fact-checkers, and coordinated inauthentic behaviours (CIBs) are also removed by our Trust and Safety team.</p>	<p>Microsoft Advertising partners with third parties as sources for strategic intelligence on domains. Microsoft Advertising actions domains, based in part on these sources evaluations as foreign influence related or non-compliant.</p> <p>Microsoft Advertising is a member and an active participant in several trade groups, including the IAB and EDAA.</p> <p>As part of the broader Microsoft engagements, Microsoft Advertising participates in threat exchange discussions with industry peers and trusted third parties which increase the effectiveness of our enforcement actions.</p>

	<p>LinkedIn, along with its parent company, Microsoft, is heavily involved in threat exchanges. These threat exchanges take various forms, such as: 1) regular discussion amongst industry peers to discuss high-level trends and campaigns; and, 2) one-on-one engagement with individual peer companies to discuss TTPs and IOCs. This exchange of information leads to a better understanding of the incentives of sophisticated and well-funded threat actors and how they evolve their TTPs to achieve those goals, which assists us in their identification and removal.</p> <p>LinkedIn always stands ready to receive and investigate any leads we receive from peers and other external stakeholders. In addition to one-on-one engagement with peers, we also consume intelligence from vendors and investigate any TTPs and IOCs made available in peer disclosures. In turn, we also regularly release information about disinformation on our platform in publicly-available transparency reports and blog posts.</p>	
Measure 3.2	LinkedIn	Microsoft Advertising
QRE 3.2.1	Please see the response to QRE 3.1.1.	Please see the response to QRE 3.1.1.
Measure 3.3	LinkedIn	Microsoft Advertising
QRE 3.3.1	Please see the response to QRE 3.1.1. In addition, as discussed in response to QRE 1.6.1, LinkedIn partners with companies including Integral Ad Science and DoubleVerify to help evaluate and filter advertising inventory on LinkedIn Audience Network publisher sites that falls short of standards, such as brand safety floors.	Please see the response to QRE 3.1.1.

III. Political Advertising

Commitments 4 - 13

III. Political Advertising			
Commitment 4			
Relevant Signatories commit to adopt a common definition of “political and issue advertising”.			
	C.4	M 4.1	M 4.2
We signed up to the following measures of this commitment:	LinkedIn Microsoft Advertising	LinkedIn Microsoft Advertising	LinkedIn Microsoft Advertising

	LinkedIn	Microsoft Advertising
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	No
If yes, list these implementation measures here [short bullet points].	New Implementation Measures Not applicable.	New Implementation Measures Not applicable.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No	No
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures Not applicable.	Planned Implementation Measures Not applicable.

Measure 4.1	LinkedIn	Microsoft Advertising
Measure 4.2	LinkedIn	Microsoft Advertising
QRE 4.1.1 (for measures 4.1 and 4.2)	LinkedIn’s Advertising Policies do not allow political advertising, and LinkedIn has not allowed political advertising since 2018.	Microsoft Advertising policies prohibit ads for election-related content, political candidates, parties, ballot measures and political fundraising

	<p>Among other things, LinkedIn Advertising policies prohibit “ads advocating for or against a particular candidate, party, or ballot proposition or otherwise intended to influence an election outcome” and “ads fundraising for or by political candidates, parties, political action committees or similar organisations, or ballot propositions.” In addition, LinkedIn’s Advertising Policies prohibit certain types of advertisements that might be considered issue based. For example, “ads exploiting a sensitive political issue even if the advertiser has no explicit political agenda” are also prohibited.</p>	<p>globally. Similarly, ads aimed at fundraising for political candidates, parties, political action committees (“PACs”), and ballot measures also are barred. All Microsoft and third-party services that rely on Microsoft Advertising to serve advertisements on their platforms benefit from these robustly enforced set of policies.</p> <p>Furthermore, Microsoft prohibits political advertising across Microsoft media properties and platforms. Microsoft Advertising’s policies also prohibit certain types of advertisements that might be considered issue-based. More specifically, “advertising that exploits political agendas, sensitive political issues or uses ‘hot button’ political issues or names of prominent politicians is not allowed regardless of whether the advertiser has a political agenda,” and “advertising that exploits sensitive political [or religious] issues for commercial gain or promote extreme political [or extreme religious] agendas or any known associations with hate, criminal or terrorist activities” is also prohibited.</p> <p>As stated in our revised policies, “We may use a combination of internal signals and trusted third-party data or information sources to reject, block, or take down ads or sites that contain disinformation or send traffic to pages containing disinformation.”</p> <p>Microsoft Advertising partners with third parties as sources for strategic intelligence on domains. Microsoft Advertising actions domains, based in part on these sources evaluations as foreign influence related or non-compliant.</p> <p>See here: Microsoft Advertising - Restricted Content - Political Content and Microsoft Advertising – Restricted Content - Religious Content</p>
QRE 4.1.2 (for measures 4.1 and 4.2)	Microsoft looks forward to the full entry into application of the Regulation on Transparency and Targeting of Political Advertising	Microsoft looks forward to the full entry into application of the Regulation on Transparency and Targeting of Political Advertising and the associated

	and the associated upcoming common guidance to be issued in accordance with Art. 8.2 of the Regulation.	upcoming common guidance to be issued in accordance with Art. 8.2 of the Regulation.
--	---	--

III. Political Advertising

Commitment 5

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

	C.5	M 5.1
We signed up to the following measures of this commitment:	LinkedIn Microsoft Advertising	LinkedIn Microsoft Advertising

	LinkedIn	Microsoft Advertising
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	No
If yes, list these implementation measures here [short bullet points].	New Implementation Measures Not applicable.	New Implementation Measures Not applicable.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No	No
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures Not applicable as LinkedIn currently prohibits all political	Planned Implementation Measures Not applicable as Microsoft Advertising currently prohibits all political advertising, as outlined under QRE 5.1.1.

	advertising, as outlined under QRE 5.1.1.	
--	---	--

Measure 5.1	LinkedIn	Microsoft Advertising
QRE 5.1.1	<p>LinkedIn's Advertising Policies do not allow political advertising, and LinkedIn has not allowed political advertising since 2018.</p> <p>Among other things, LinkedIn Advertising policies prohibit “ads advocating for or against a particular candidate, party, or ballot proposition or otherwise intended to influence an election outcome” and “ads fundraising for or by political candidates, parties, political action committees or similar organisations, or ballot propositions.” In addition, LinkedIn's Advertising Policies prohibit certain types of advertisements that might be considered issue based. For example, “ads exploiting a sensitive political issue even if the advertiser has no explicit political agenda” are also prohibited.</p>	<p>Microsoft Advertising policies prohibit ads for election-related content, political candidates, parties, ballot measures and political fundraising globally; similarly, ads aimed at fundraising for political candidates, parties, political action committees (“PACs”), and ballot measures also are barred. All Microsoft and third-party services that rely on Microsoft Advertising to serve advertisements on their platforms benefit from these robustly enforced set of policies.</p> <p>Furthermore, Microsoft prohibits political advertising across Microsoft media properties and platforms. Microsoft Advertising's policies also prohibit certain types of advertisements that might be considered issue-based. More specifically, “advertising that exploits political agendas, sensitive political issues or uses ‘hot button’ political issues or names of prominent politicians is not allowed regardless of whether the advertiser has a political agenda,” and “advertising that exploits sensitive political [or religious] issues for commercial gain or promote extreme political or extreme religious agendas or any known associations with hate, criminal or terrorist activities” is also prohibited.</p> <p>See here: Microsoft Advertising - Restricted Content - Political content and Microsoft Advertising – Restricted Content - Religious Content</p>

III. Political Advertising						
Commitment 6						
Relevant Signatories commit to make political or issue ads clearly labelled and distinguishable as paid-for content in a way that allows users to understand that the content displayed contains political or issue advertising						
	C.6	M 6.1	M 6.2	M 6.3	M 6.4	M 6.5
We signed up to the following measures of this commitment:	Commitment 6 is not relevant or pertinent for LinkedIn and Microsoft Advertising as they do not allow political or issue-based advertising as set out in more detail under measure 5.1.	N/A	N/A	N/A	N/A	N/A

III. Political Advertising					
Commitment 7					
Relevant Signatories commit to put proportionate and appropriate identity verification systems in place for sponsors and providers of advertising services acting on behalf of sponsors placing political or issue ads. Relevant signatories will make sure that labelling and user-facing transparency requirements are met before allowing placement of such ads.					
	C.7	M 7.1	M 7.2	M 7.3	M 7.4
We signed up to the following measures of this commitment:	LinkedIn Microsoft Advertising	N/A	N/A	LinkedIn Microsoft Advertising	N/A

	LinkedIn	Microsoft Advertising
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	No
If yes, list these implementation measures here [short bullet points].	New Implementation Measures Not applicable	New Implementation Measures Not applicable

Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No	No
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures Not applicable	Planned Implementation Measures Not applicable

Measure 7.3	LinkedIn	Microsoft Advertising
QRE 7.3.1	<p>As set out in QRE 5.1.1, LinkedIn's Advertising Policies prohibit political advertising. Before submitting a campaign, customers must agree that their ad complies with LinkedIn's policies.</p> <p>As detailed in QRE 2.3.1, LinkedIn has implemented both automated and manual systems to help ensure that advertising on the platform complies with its Advertising Policies, and that ads that do not comply with its policies are removed. These enforcement systems apply equally to prohibited political advertising, as well as other violations of LinkedIn's Advertising Policies.</p> <p>In addition to LinkedIn's pre-emptive enforcement, LinkedIn members may also report ads that they believe violate LinkedIn's advertising policies, and when members report ads LinkedIn's advertising review team reviews them. To report an ad, members can click on the three-dot icon in the upper right-hand corner of every ad and select the "Hide or report this ad" option.</p>	<p>As set out in QRE 5.1.1, Microsoft Advertising prohibits ads for election-related content, political candidates, parties, ballot measures and political fundraising globally; similarly, ads aimed at fundraising for political candidates, parties, political action committees ("PACs"), and ballot measures also are barred. All Microsoft and third-party services that rely on Microsoft Advertising to serve advertisements on their platforms benefit from these robustly enforced set of policies.</p> <p>Furthermore, Microsoft Advertising's policies also prohibit certain types of advertisements that might be considered issue-based. More specifically, "advertising that exploits political agendas, sensitive political issues or uses 'hot button' political issues or names of prominent politicians is not allowed regardless of whether the advertiser has a political agenda," and "advertising that exploits sensitive political [or religious] issues for commercial gain or promote extreme political or extreme religious agendas or any known associations with hate, criminal or terrorist activities" is also prohibited. In addition, to comply with local laws in Canada and France, Microsoft Advertising has prohibited advertising content related to debates of general interest linked to an electoral campaign in those jurisdictions.</p> <p>See here: Microsoft Advertising - Restricted Content - Political content and Microsoft Advertising - Restricted Content - Religious Content</p>

QRE 7.3.2	As set out in QRE 5.1.1, LinkedIn's Advertising Policies prohibit political advertising. Ads that do not comply with LinkedIn's Advertising Policies are removed.	<p>Microsoft Advertising does not offer its advertising services to customers or partners that may promote political content. For example, a political party would be made aware by our customer support team that it cannot run political ads campaigns through our ad network.</p> <p>Microsoft Advertising employs dedicated operational support and engineering resources to enforce restrictions on political advertising using a combination of proactive and reactive mechanisms. On the proactive side, Microsoft Advertising has implemented several processes designed to identify and block political ads from showing across its advertising network, including restrictions on certain terms and from certain domains. For example, we compile a list of terms comprised of known political parties, candidates, and ballot measures and block any ads that may be otherwise shown on a search engine search for such terms. On the reactive side, if Microsoft Advertising becomes aware that an ad suspected of violating its policies is being served to our publishers—for instance, because a user flagged that ad to our customer support team—the offending ad is promptly reviewed. If it violates our policies, we will take it down. Users can report advertising that may be in violation of the Microsoft Advertising policies through the publisher-specific reporting form or via this form: Low quality ad submission & escalation - Microsoft Advertising</p> <p>The above actions apply across all the websites that use Microsoft Advertising to serve ads on their properties, whether owned and operated by Microsoft (like Bing) or third-party websites.</p>
------------------	---	---

III. Political Advertising			
Commitment 8			
Relevant Signatories commit to provide transparency information to users about the political or issue ads they see on their service.			
		M 8.1	M 8.2
We signed up to the following measures of this commitment:	Commitment 8 is not relevant or pertinent for LinkedIn and Microsoft Advertising as they do not allow political or issue-based advertising as set out in more detail under measure 5.1.	N/A	N/A

III. Political Advertising			
Commitment 9			
Relevant Signatories commit to provide users with clear, comprehensible, comprehensive information about why they are seeing a political or issue ad.			
	C.9	M 9.1	M 9.2
We signed up to the following measures of this commitment:	Commitment 9 is not relevant or pertinent for LinkedIn and Microsoft Advertising as they do not allow political or issue-based advertising as set out in more detail under measure 5.1.	N/A	N/A

III. Political Advertising			
Commitment 10			
Relevant Signatories commit to maintain repositories of political or issue advertising and ensure their currentness, completeness, usability and quality, such that they contain all political and issue advertising served, along with the necessary information to comply with their legal obligations and with transparency commitments under this Code.			
	C.10	M 10.1	M 10.2
We signed up to the following measures of this commitment:	Commitment 10 is not relevant or pertinent for LinkedIn and Microsoft Advertising as they do not allow political or issue-based advertising as set out in more detail under measure 5.1.	N/A	N/A

III. Political Advertising					
Commitment 11					
Relevant Signatories commit to provide application programming interfaces (APIs) or other interfaces enabling users and researchers to perform customised searches within their ad repositories of political or issue advertising and to include a set of minimum functionalities as well as a set of minimum search criteria for the application of APIs or other interfaces.”					
	C.11	M 11.1	M 11.2	M 11.3	M 11.4
	Commitment 11 is not relevant or pertinent for LinkedIn and Microsoft Advertising as they do not allow political or issue-based advertising as set out in more detail under measure 5.1.	N/A	N/A	N/A	N/A

III. Political Advertising					
Commitment 12					
Relevant Signatories commit to increase oversight of political and issue advertising and constructively assist, as appropriate, in the creation, implementation and improvement of political or issue advertising policies and practices.					
	C.12	M 12.1	M 12.2	M 12.3	
We signed up to the following measures of this commitment:	Commitment 12 is not relevant or pertinent for LinkedIn and Microsoft Advertising as they do not allow political or issue-based advertising as set out in more detail under measure 5.1.	N/A	N/A	N/A	

III. Political Advertising					
Commitment 13					
Relevant Signatories agree to engage in ongoing monitoring and research to understand and respond to risks related to Disinformation in political or issue advertising.					
	C.13	M 13.1	M 13.2	M 13.3	
We signed up to the following measures of this commitment:	Commitment 13 is not relevant or pertinent for LinkedIn and Microsoft Advertising as they do not allow political or issue-based advertising as set out in more detail under measure 5.1.	N/A	N/A	N/A	

IV. Integrity of Services

Commitments 14 - 16

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

--	--	--	--	--

	C.14	M 14.1	M 14.2	M 14.3
We signed up to the following measures of this commitment:	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search

	LinkedIn	Bing Search
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	Yes
If yes, list these implementation measures here [short bullet points].	<p>New Implementation Measures</p> <p>Not applicable</p>	<p>New Implementation Measures</p> <p>During the reporting period Microsoft continued piloting Content Integrity Tools, which allowed users to add content credentials to their own authentic content. Designed as a pilot program primarily to support the 2024 election cycle and gather feedback about Content Credentials-enabled tools, during the reporting period of this report, the tools were available to political campaigns in the EU, as well as to elections authorities and select news media organizations in the EU and globally. These tools included a partnership and collaboration with fellow Tech Accord signatory, TruePic. Announced in April 2024, this collaboration leveraged TruePic's mobile camera SDK enabling campaign, election, and media participants to capture</p>

		authentic images, videos and audio directly from a vetted and secure device. Called the "Content Integrity Capture App" (an app that makes it easy to directly capture images with C2PA enabled signing) launched for both Android and Apple and can be used by participants in the Content Integrity Tools pilot program.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No	No
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures Not applicable	Planned Implementation Measures Not applicable

Measure 14.1	LinkedIn	Bing Search
QRE 14.1.1	<p>LinkedIn's User Agreement (in particular section 8 <i>LinkedIn "Dos and Don'ts"</i>) and our Professional Community Policies - which are accepted by every member when joining LinkedIn - detail the impermissible manipulative behaviours and practices that are prohibited on our platform. Fake accounts, misinformation, and inauthentic content are not allowed, and we take active steps to remove it from our platform.</p> <p>LinkedIn provides additional specific examples of false and misleading content that violates its policy via a Help Center article on False or Misleading Content.</p>	<p>Bing Search is an online search engine, the primary purpose of which is to provide a searchable index of webpages available on the internet to help users find the content they are looking for. Bing Search does not host the content or control the operation, content, or design of indexed websites. Users come to Bing Search with a specific research topic in mind and expect Bing to provide links to the most relevant and authoritative third-party websites on the Internet that are responsive to their search terms. Bing Search does not allow users to post and share content or otherwise enable content to go "viral" through user-to-user exchanges of information on Bing.</p> <p>As such, addressing misinformation in organic search results often requires a different approach than may be appropriate for other types of online services. The majority of the TTPs (namely, TTPs 1-9 and 11-12) are more</p>

	<p>pertinent to social media or account-driven services in that they specifically relate to user accounts, subscribers/followers, inauthentic coordination, influencers, or targeting users of a service, account hijacking, etc., and thus are not relevant to search engines.</p> <p>The highest potential for abuse in web search arises under TTP 10, which involves “use of deceptive practices to deceive/manipulate platform algorithms, such as by exploiting data voids, spam tactics, or keyword stuffing.” Therefore, relevant Bing Search policies and practices that help combat manipulative behaviors primarily address TTP Number 10.</p> <p>Although as a search engine Bing does not have any control over third party websites appearing in search results, Bing’s ranking algorithms, spam policies, and other safeguards described below can also address and mitigate the risks arising from malicious websites that use other TTPs attempting to manipulate our search engine rankings. For example, pages employing social media schemes (e.g., fake followers – TTP 3), using inauthentic domains (TTP 4), or keyword stuffing (TTP 9) are considered abusive practices that are addressed in Bing’s ranking system and Webmaster Guidelines. In addition, in connection with generative AI features, Microsoft has implemented measures intended to address TTP No. 7 (related to deceptive deepfakes), which are discussed in more detail below.</p> <p>Bing’s primary mechanism for combatting manipulative behaviors in search results is via its ranking algorithms and systems designed to identify and combat attempts to abuse search engine optimization techniques (i.e., spam). Bing Search describes the main parameters of its ranking systems in depth in How Bing Delivers Search Results. Abusive techniques and examples of prohibited SEO activities are described in more detail in the Bing Webmaster Guidelines.</p> <p>As described in these documents, Bing’s ranking algorithms are designed to identify and prioritize high quality, highly authoritative content available</p>
--	---

		<p>online that is relevant to the user's query and to prevent abusive search engine optimization techniques (spam).</p> <p>One of the key ranking techniques Bing uses to prevent low quality or deceptive websites from returning high in search results is through the "quality and credibility" score. Determining the quality and credibility (QC) of a website includes evaluating the clarity of purpose of the site, its usability, and presentation. QC also consists of an evaluation of the page's "authority", which includes factors such as:</p> <ul style="list-style-type: none"> ▪ Reputation: What types of other websites link to the site? A well-known news site is considered to have a higher reputation than a brand-new blog. ▪ Level of discourse: Is the purpose of the content solely to cause harm to individuals or groups of people? For example, a site that promotes violence or resorts to name-calling or bullying will be considered to have a low level of discourse, and therefore lower authority, than a balanced news article. ▪ Level of distortion: How well does the site differentiate fact from opinion? A site that is clearly labeled as satire or parody will have more authority than one that tries to obscure its intent. ▪ Origination and transparency of the ownership: Is the site reporting first-hand information, or does it summarize or republish content from others? If the site doesn't publish original content, do they attribute the source? A first-hand account published on a personal blog could have more authority than unsourced content. <p>In addition to its ranking algorithms, Bing Search's general abuse/spam policies prohibit certain practices intended to manipulate or deceive the Bing Search algorithms, including those that could be employed by malicious actors in the spread of disinformation. Pursuant to the Webmaster Guidelines, Bing may take action on websites employing spam tactics (such as social media schemes, keyword stuffing, malicious behavior, cloaking, link</p>
--	--	---

	<p>schemes, or misleading structured data markups) or that otherwise violate the Webmaster Guidelines, including by applying ranking penalties (such as demoting a website) or delisting a website from the index.</p> <p>Note that it is not feasible to distinguish between general spam tactics and spam tactics employed by malicious actors specifically for the purpose of spreading disinformation. Therefore, Bing Search has not presented data on the amount of spam detected and actioned under its policies since these figures are indicative of actions taken toward spam overall and presently cannot be used to provide an accurate assessment of whether it pertains to spam used in connection with disinformation campaigns or spam used for another purpose (e.g., phishing).</p> <p><u>Generative AI Features</u></p> <p>During the Reporting Period, the nature of Bing generative AI experiences evolved. In October 2024, Microsoft launched a separate, standalone consumer service known as Microsoft Copilot at copilot.microsoft.com, which offers conversational experiences powered by generative AI, and the Copilot in Bing (formerly known as Bing Chat) generative AI experience was phased out. Bing continues to offer generative AI experiences, such as Bing Image Creator and Bing Generative Search, which was launched this Reporting Period. Bing Generative Search utilizes AI to deliver a unique experience by not only optimizing search results but presenting information in a user-friendly, cohesive layout. Results also include citations and links that enable users to explore further and evaluate websites for themselves. For AI-powered experiences, Bing has partnered closely with Microsoft's Responsible AI team to proactively address AI-related risks and continues to evolve these features based on user and external stakeholder feedback. Bing generative AI experiences continue to rely on the same infrastructure and mitigations previously discussed in Microsoft's last report.</p> <p>Bing Generative Search's primary functionality is, like traditional Bing search, to provide users with links to third party content responsive to their search</p>
--	--

	<p>queries. As such, the ranking algorithms and spam/abuse policies described above continue to be Bing's primary defense against manipulation and abuse, supplemented by interventions designed specifically to address manipulation in generative AI features. As to answers triggering creative inspiration, Microsoft has worked continuously to improve and adjust safety mitigations, policies, and user experiences within Bing's generative AI experiences to minimize the risk they may be used for manipulative purposes. Additional information on how Microsoft approached responsible AI in Bing's generative AI experiences is available How Bing Delivers Search Results.</p> <p>TTP 10 remains the most relevant TTP to Bing's generative AI experiences, as users cannot post or share content directly on the Bing service. In addition, Microsoft undertakes specific mitigations to address TTP 7 given the risks that users may attempt to use generative AI to create deepfakes or manipulated media to spread disinformation. Although Bing does not have the ability to monitor third party platforms for publication of content created through Bing's services, Bing has implemented safeguards to help to minimize the risk that bad actors can use Bing generative AI experiences to create mis/disinformation.</p> <p>Microsoft's Copilot AI Experiences Terms (applicable to Copilot in Bing through October 2024) and Bing's Image Creator Terms of Use (referred to here as "Supplemental Terms") advise users on prohibited conduct and content. These Supplemental Terms primarily address TTPs No. 10 and 7 by restricting attempts to create or spread mis/disinformation or deceptive images using Bing's generative AI experiences. Users that violate the Supplemental Terms and Code of Conduct may be suspended from the service. In addition, Bing's generative AI experiences work to prevent generation of problematic text or images by blocking user prompts that (i) violate the Code of Conduct or (ii) are likely to lead to creation of material that violates the Code of Conduct. Repeated attempts to produce prohibited</p>
--	---

		<p>content or other violations of the Code of Conduct may also result in service or account suspension.</p> <p>For further information as to how Bing Search and Bing's generative AI experiences implement these policies see QRE 14.1.2.</p>
QRE 14.1.2	<p>LinkedIn works with numerous partners to facilitate the flow of information to tackle purveyors of disinformation, including disinformation spread by state-sponsored and institutional actors.</p> <p>LinkedIn maintains an internal Trust and Safety team composed of threat investigators and intelligence analysts to address disinformation. This team works with peers and other stakeholders, including our Artificial Intelligence modeling team, to identify and remove nation-state actors and coordinated inauthentic campaigns. LinkedIn conducts investigations into election-related influence operations and nation-state targeting including continued information sharing on threats with industry peers and Law Enforcement on a regular basis. LinkedIn works with peer companies and other stakeholders to receive and share indicators related to fake accounts created by state-sponsored actors, such as confirmed Tactics, Techniques, and Protocols (TTPs) and Indicators of Compromise (IOC). This exchange of information leads to a better understanding of the incentives of sophisticated and well-funded threat actors and how they evolve their TTPs to achieve those goals, which assists LinkedIn in their identification and removal. Any associated disinformation content is verified by our internal or external fact-checkers as needed, and coordinated inauthentic behaviours (CIBs) are also removed by our Trust and Safety team.</p> <p>LinkedIn, along with its parent company, Microsoft, is heavily involved in threat exchanges. These threat exchanges take various forms, such as: 1) regular discussion amongst industry peers to discuss high-level trends and campaigns; and, 2) one-on-one</p>	<p>As discussed under QRE 14.1.1, TTP No. 10 tends to be the primary mechanism for manipulation and abuse in the context of search engines and is addressed through Bing's ranking systems and abuse policies (for both traditional search and Bing's generative AI experiences).</p> <p>Blocking content in organic search results based solely on the truth or falsity of the content can raise significant concerns relating to fundamental rights of freedom of expression and the freedom to receive and impart information. Instead of blocking access to content to address these TTPs, Bing Search focuses on ranking its organic search results so that trusted, authoritative news and information appears first and provides tools to help its users evaluate the trustworthiness of certain sites and ensure they are not misled or harmed by the content that appears in search results. Bing presumes the user seeks high quality, authoritative content unless the user clearly indicates an intent to research low quality content. Bing Search takes actions to promote high authority, high quality content and thereby reduce the impact of misinformation appearing in Bing Search results. This includes Bing Search's continued improvement of its ranking algorithms to ensure that authoritative, relevant content is returned at the top of search results, regular review and actioning of disinformation threat intelligence, partnership with third party information intelligence and media literacy organizations, contributing to and supporting the research community, and enforcement of clear policies concerning the use of manipulative tactics on Bing Search, among other initiatives described elsewhere in this report.</p> <p>Although the Bing Search algorithm endeavors to prioritize relevance, quality, and credibility, in some cases Bing Search identifies threats arising from emerging or evolving world events and/or activities by external actors</p>

	<p>engagement with individual peer companies to discuss TTPs and IOCs. This exchange of information leads to a better understanding of the incentives of sophisticated and well-funded threat actors and how they evolve their TTPs to achieve those goals, which assists us in their identification and removal.</p> <p>LinkedIn always stands ready to receive and investigate any leads we receive from peers and other external stakeholders. In addition to one-on-one engagement with peers, we also consume intelligence from vendors and investigate any TTPs and IOCs made available in peer disclosures. In turn, we also regularly release information about policy-violating content on our platform in publicly available transparency reports and blog posts, including for example How We're Protecting Members From Fake Profiles, Automated Fake Account Detection, and An Update on How We Keep Members Safe. The LinkedIn Community Report also describes actions we take on content that violates our Professional Community Policies and User Agreement. It is published twice per year and covers the global detection of fake accounts, spam and scams, content violations and copyright infringements. The most recent reporting period covered 1 January to 30 June 2024. LinkedIn Ireland Unlimited Company – the provider of LinkedIn's services in the EU – has been designated by the European Commission as a very large online platform and, therefore, pursuant to its obligations under Article 42 of the Digital Services Act, publishes Transparency Reports covering the EU every 6 months, with the most recent report published in February 2025.</p>	<p>that attempt to undermine the efficacy of its algorithms. When this happens, Bing Search employs “defensive search” strategies and interventions to counteract threats and TTPs in accordance with its trustworthy search principles (which are discussed in further detail in the How Bing Delivers Search Results).</p> <p>“Defensive search interventions” may include algorithmic interventions (such as authority signal boost in ranking or demotions of a website), restricting autosuggest or related search terms to avoid directing users to problematic queries, prioritizing additional features promoting high authority information (e.g., Answers or Public Service Announcements), and in limited cases manual interventions for individual reported issues or broader areas more prone to misinformation or disinformation. Bing actively monitors manipulation trends in identified high-risk areas and deploys mitigation methods as needed to ensure users are provided with high quality, high authority search results.</p> <p>In addition to defensive search, Bing Search regularly monitors for other violations of its Webmaster Guidelines, including attempts to manipulate the Bing Search algorithm through prohibited practices such as cloaking, link spamming, keyword stuffing, and phishing. Bing Search dedicates meaningful resources to maintaining the integrity of the platform, promoting high authority, relevant results, and reducing spam (including spam aimed at distributing low authority information and manipulative content). Bing Search utilizes a combination of human intervention and AI-driven analysis to regularly review, detect, and address spam tactics occurring on Bing Search. When Bing Search detects websites deploying manipulative techniques or engaging in spam tactics, those websites may incur ranking penalties or be removed from the Bing Search index altogether.</p>
--	---	---

	<p>Microsoft also works to identify and track nation-state information operations targeting democracies across the world and works with a number of trusted third-party partners for early indicators of narratives, hashtags, or information operations that can be leveraged to inform early detection and defensive search strategies. Through Microsoft's Democracy Forward team and the Microsoft Threat Assessment Center (MTAC), Microsoft also offers mediums for election authorities, including in the EU and EEA Member States, to have lines of communication with Microsoft to identify possible foreign information operations targeting elections.</p> <p>The above measures also apply to Bing's generative AI experiences. responses to user prompts are "grounded" on high authority content from the web (except in certain creative use cases), which are based on the same ranking algorithms and moderation infrastructure that are used by Bing's traditional web search, and, as such, benefit from Bing's longstanding safety infrastructure described above. Nonetheless, Microsoft recognizes that generative AI technology may also raise novel risks and possibilities of harm that are not present in traditional web search and has supplemented its existing threat identification and mitigation processes with additional risk assessments and mitigation processes based on Microsoft's Responsible AI program.</p> <p>Microsoft's Responsible AI program is designed to identify potential harms, measure their propensity to occur, and build mitigations to address them. Guided by its Responsible AI Standard, Microsoft identifies, measures, and mitigates potential harms and misuse of new generative AI experiences while securing the transformative and beneficial uses that these tools provide. , Microsoft has implemented a range of safety mitigations to help address, among other things, impermissible content, behaviours, and other TTPs that could potentially be used to create or spread misinformation.</p>
--	--

		<p>Below are several examples of Microsoft’s iterative approach to identify, measure, and mitigate potential harms, including the spread of misinformation.</p> <p>- Pre-launch and ongoing testing. Before launching Bing’s generative AI experiences, Microsoft conducted “red team” testing. A multidisciplinary team of experts evaluated how well the system responded when pressed to produce harmful responses, surface potential avenues for misuse, and identify capabilities and limitations. Post-release, generative AI experiences are integrated into Microsoft engineering organizations’ existing production measurement and testing infrastructure. More information on Microsoft’s approach to red-team testing is available at Microsoft AI Red Team building future of safer AI Microsoft Security Blog.</p> <p>- Classifiers, Metaprompting, and Filtering Interventions: Microsoft has created special mitigations in the form of “classifiers” and “metaprompting” to help reduce the risk of certain harms and misuse of generative AI features. <i>Classifiers</i> classify text to flag different types of potentially harmful content in search queries, chat prompts, or generated responses. Microsoft uses AI-based classifiers and content filters, which apply to all search results and relevant features; it also designed additional prompt classifiers and content filters specifically to address possible harms raised by new generative AI features.. Flags lead to potential mitigations, such as not returning generated content to the user, diverting the user to a different topic, or redirecting the user to traditional search. Metaprompting involves giving instructions to the model to guide its behavior, including so that the system behaves in accordance with Microsoft’s AI Principles and user expectations. Microsoft has also implemented additional filtering and classifiers to prevent chat responses from returning what Bing considers “low authority” content as part of an answer and to help address impermissible content, behaviours, and other TTPs (e.g., TTP No. 7) that could potentially be used to create or spread misinformation.</p>
--	--	---

	<ul style="list-style-type: none">- Content Provenance Tools. Microsoft also makes it clear that images created in Bing Image Creator (and Copilot in Bing prior to its phase out) are AI-generated by including content provenance information in each image. These content provenance features use cryptographic methods to mark and sign AI-generated content with metadata about its source and history. The invisible digital watermark feature shows the source, time, and date of original creation, and this information cannot be altered. Providing clear indications of image provenance helps reduce the risk of deepfakes (e.g., TTP No. 7) and helps users identify when an image was generated with the assistance of Microsoft generative AI tools. Microsoft has partnered with other industry leaders to create the Coalition for Content Provenance and Authenticity (C2PA) standards body to help develop and apply content provenance standards across the industry.- Expanded and Prominent Reporting Functionality. Bing's generative AI experiences allow users to submit feedback and report their concerns, which are then reviewed by Microsoft's operations teams. Microsoft has made it easy for users to report problematic content they encounter while using generative AI features in Bing by including a "Feedback" portal on the footer of every Bing page, with direct links to its "Report a Concern" tool.- Regular Improvements Based on Real World Usage. Microsoft continues to make changes to Bing generative AI experiences regularly to improve product performance, update existing mitigations, and implement new mitigations in response to our learnings based on real-world usage of the product.- Operations and incident response. Bing also uses Microsoft's ongoing monitoring and operational processes to address when Bing's generative AI features receive signals or a report indicating possible misuse or violations of the terms of use.
--	---

		<p>- Cooperation with Industry Partners. The third-party content that grounds Bing's generative AI experiences relies on the same ranking algorithms and defensive interventions that power traditional Bing search, including reliance on signals of page authority that Bing receives from its third-party partners and fact-checks using the ClaimReview protocol.</p> <p>Our approach to identifying, measuring, and mitigating harms will continue to evolve as we learn more, and we continue to make improvements based on feedback from users, civil society groups, and other third-party stakeholders.</p> <p>Microsoft also maintains a web page – Microsoft-2024 Elections – where political candidates and election authorities can report alleged deepfakes of themselves or the election process on Microsoft platforms to Microsoft.</p> <p>See also response to QRE 14.1.1.</p>
Measure 14.2	LinkedIn	Bing Search
QRE 14.2.1	<p>LinkedIn's Professional Community Policies prohibit misinformation and misinformation is removed from the LinkedIn platform. Where LinkedIn removes such content pursuant to our false and misleading content policies, LinkedIn notifies members of the action taken. Members that repeatedly post misinformation are permanently restricted. State-sponsored attempts to post misinformation, if any, are removed.</p> <p>Further, LinkedIn's professional focus shapes the type of content we see on platform. People tend to say things differently when their colleagues and employer are watching. Accordingly, our members don't tend to use LinkedIn to engage in the mass dissemination of misinformation, and bad actors generally need to create fake accounts to peddle misinformation.</p>	<p>The Webmaster Guidelines – and related defensive search and spam interventions – are global policies that are enforced globally by Bing Search, including in EU Member States. Websites that appear in Bing search results (in traditional search or in generative AI chat) are not hosted by Bing Search and, as such, Bing Search has limited information about the hosting location of these third-party websites. When addressing spam activity, Bing Search takes action at the global level (which necessarily carry through to Copilot AI features reliant on the Bing search index) to benefit Bing Search users in all countries (including EU Member States). Bing Search's defensive search interventions are also applied at a global level (thereby encompassing all EU member states) and automatically applied to queries searched in all EU languages. Metrics on defensive search interventions are provided in SLI 14.2.1.</p>

	<p>To ensure their content reaches a large audience, bad actors need to either connect with real members or post content that real members will like—both of which are hard to achieve on LinkedIn given our professional focus. The mass dissemination of false information, as well as artificial traffic and engagement, therefore, requires the mass creation of fake accounts, which we have various defences to prevent and limit.</p> <p>To evolve to the ever-changing threat landscape, our team continually invests in new technologies for combating inauthentic behaviour on the platform. We are investing in artificial intelligence technologies such as advanced network algorithms that detect communities of fake accounts through similarities in their content and behaviour, computer vision and natural language processing algorithms for detecting AI-generated elements in fake profiles, anomaly detection of risky behaviours, and deep learning models for detecting sequences of activity that are associated with abusive automation. As noted in our most recent global Transparency Report, in the period 1 January to 30 June 2024, LinkedIn blocked or removed approximately 86 million fake accounts. Our automated defenses blocked 94.6% of the fake accounts we stopped during that period, with the remaining 5.4% stopped by our manual investigations and restrictions. 99.7% of the fake accounts were stopped proactively, before a member report.</p> <p>To respond to the ever-changing threat landscape, LinkedIn's teams continually invest in new technologies for combating inauthentic behavior on the platform. LinkedIn committed to the Tech Accord to Combat Deceptive Use of AI in 2024 Elections. Aligned with this commitment, LinkedIn is investing in AI technologies such as advanced network algorithms that detect communities of fake</p>	<p>See also responses to QRE 14.1.1-2.</p>
--	--	--

	<p>accounts through similarities in their content and behavior; computer vision and natural language processing algorithms for detecting AI-generated elements in fake Profiles such as deep fakes; anomaly detection of risky behaviors; and deep learning models for detecting sequences of activity that are associated with abusive automation. LinkedIn has also adopted the Coalition for Content Provenance and Authenticity's industry-leading "Content Credentials" technology (C2PA) to include metadata labeling, including data about whether content is created using AI, on content containing the C2PA technology. Furthermore, LinkedIn acts vigilantly to maintain the integrity of all accounts and to ward off false account activity:</p> <ul style="list-style-type: none"> - Establishing metrics for when election-related conversations, violations, or operational capacity breach a threshold and require additional support - Maintaining a dedicated Anti-Abuse team to research emerging trends and key risks and develop tools to address them - Using AI to detect inauthentic activity and communities of fake accounts - Using automated systems to detect and block automated activity - Imposing limits on certain categories of activity commonly engaged in by bad actors - Conducting manual investigation and restriction of accounts engaged in automated activity - Using third party fact checkers during the human content review process - Conducting hash matching for known instances of deepfake content - Maintaining 24/7 escalation paths to address any emerging issues 	
--	---	--

	<p>LinkedIn has reported available metrics at SLI 14.2.1 in respect of the following TTPs:</p> <ul style="list-style-type: none"> - TTP 1: Creation of inauthentic accounts or botnets (which may include automated, partially automated, or nonautomated accounts) - TTP 2: Use of fake / inauthentic reactions (e.g. likes, up votes, comments) - TTP 3: Use of fake followers or subscribers - TTP 4: Creation of inauthentic pages, groups, chat groups, fora, or domains <p>LinkedIn has also reported metrics for SLI 14.2.2 in respect of TTP 1 and TTP 4.</p> <p>LinkedIn has focused its efforts on TTPs 1-4 because, as a real-identity professional network, the harm on LinkedIn is generally conducted through fake accounts. Our real members know that the content they post is viewed by their colleagues, managers, and potential business partners, and therefore they generally do not knowingly post misinformation.</p> <p>With respect to the remaining TTPs, LinkedIn is unable to reasonably ascertain the intent or provenance of such content. As discussed above, disinformation is not prevalent on LinkedIn due to the professional context of the platform. Distribution of such content through fake accounts is further hampered due to the need to create connections between the fake account and the real member. In the rare instances that such misinformation is spread through fake accounts, due to the adversarial nature of this activity, publicly disclosing details regarding the threat actor's TTPs would hurt our ability to fight against this activity. For example, reporting that</p>	
--	---	--

	<p>vulnerable recipients were not targeted may incentivize the targeting of such recipients.</p> <p>LinkedIn has and will continue to evaluate what additional metrics it could potentially include in future reporting in light of how LinkedIn's services function and are used.</p>	
--	--	--

	LinkedIn			
	SLI 14.2.1 – SLI 14.2.4			
TTP 1	<p>The table below addresses TTP 1: "Creation of inauthentic accounts or botnets (which may include automated, partially automated, or non-automated accounts)." SLI 14.2.1 reports the number of fake accounts that LinkedIn prevented from being created or restricted between 1 July - 31 December 2024, broken out by EEA Member State. The fake accounts reported are attributed to EEA Member States based on the IP address used during registration of the account. 'Number of instances of identified TTPs' and 'Number of actions taken by type' are identical given LinkedIn blocked the registration attempt or restricted the account in all instances.</p> <p>SLI 14.2.2. reports two metrics. First, the number of EEA accounts that connected to or followed the fake accounts in SLI 14.2.1 between 1 July – 31 December 2024. For example, the 194,153 fake accounts reported for Austria had a total of 3,299 EEA accounts connect to or follow them between 1 July and 31 December 2024. Whether an account qualifies as an EEA account is based on the IP address used during registration of the account. Second, the number of fake accounts in in SLI 14.2.1 that posted a feed post between 1 July – 31 December 2024. For example, of the 444,743 fake accounts prevented or restricted for Ireland, 789 posted a feed post between 1 July and 31 December 2024.</p> <p>Please note that the metrics provided below are total numbers and do not imply that these fake accounts were engaging in posting misinformation or disinformation.</p> <p>We have not reported metrics associated with this TTP where, for example, there is no meaningful metric to report (e.g., metrics for after the TTP in question, given LinkedIn removes detected misinformation and fake accounts from our platform) or LinkedIn does not have a reasonable means to compute the requested metrics.</p>			
	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4

	Nr of instances of identified TTPs	Nr of actions taken by type	Views/ impressions before action	Views/ impressions before action	Penetration and impact on genuine users	Trends on targeted audiences	Trends on narratives used	TTPs related content in relation to overall content on the service	Views/ impressions of TTP related content (in relation to overall views/ impressions on the service)	Interaction / engagement with TTP related content (in relation to overall interaction / engagement on the service)
	The number of fake accounts LinkedIn prevented or restricted between 1 July – 31 December 2024	The number of fake accounts LinkedIn prevented or restricted between 1 July – 31 December 2024	The number of EEA accounts that connected to or followed the fake accounts between 1 July – 31 December 2024	The number of fake accounts that posted a feed post between 1 July – 31 December 2024						
Member States										
Austria	194,153	194,153	3,299	710						
Belgium	344,346	344,346	5,081	1,147						
Bulgaria	140,495	140,495	2,033	549						
Croatia	53,395	53,395	1,465	236						
Cyprus	61,105	61,105	977	218						
Czech Republic	185,280	185,280	3,811	629						
Denmark	150,598	150,598	2,732	558						
Estonia	452,316	452,316	525	129						
Finland	530,752	530,752	1,701	506						
France	2,712,034	2,712,034	58,419	11,784						
Germany	1,923,995	1,923,995	35,323	9,523						
Greece	271,628	271,628	5,422	1,009						
Hungary	102,782	102,782	1,606	401						
Ireland	444,743	444,743	3,951	789						

Italy	8,365,534	8,365,534	21,848	4,535						
Latvia	468,370	468,370	1,087	230						
Lithuania	155,975	155,975	1,927	304						
Luxembourg	40,195	40,195	655	134						
Malta	31,539	31,539	587	101						
Netherlands	1,172,414	1,172,414	18,922	3,448						
Poland	597,637	597,637	13,476	2,715						
Portugal	180,022	180,022	6,676	1,448						
Romania	683,248	683,248	5,942	920						
Slovakia	84,337	4,337	1,207	266						
Slovenia	80,358	80,358	654	142						
Spain	2,046,114	2,046,114	68,945	6,128						
Sweden	518,628	518,628	6,511	1,020						
Iceland	16,166	16,166	191	36						
Liechtenstein	1,080	1,080	24	6						
Norway	104,916	104,916	1,797	413						
Total EU	21,991,993	21,991,993	274,782	49,579						
Total EEA	22,114,155	22,114,155	276,794	50,034						

TTP 2	<p>The table below addresses TTP 2: “Use of fake / inauthentic reactions (e.g. likes, up votes, comments).” The table reports the number of fake accounts reported in TTP 1 SLI 14.2.1 that reacted to, commented on, or shared (collectively, “engaged with”) a feed post between 1 July – 31 December 2024.</p> <p>The numbers of fake accounts reported below are a subset of the fake accounts reported in TTP 1 SLI 14.2.1 that engaged with a feed post between 1 July – 31 December 2024. For example, of the 194,153 fake accounts that LinkedIn prevented from being created or restricted between 1 July – 31 December 2024 in Austria (as reported in TTP 1 SLI 14.2.1), 1,148 of those accounts engaged with a feed post between 1 July – 31 December 2024.</p> <p>Please note that the metrics provided below are total numbers and do not imply that these fake accounts were engaging in posting misinformation or disinformation.</p>
--------------	---

	We have not reported metrics associated with this TTP where, for example, there is no meaningful metric to report (e.g., metrics for after the TTP in question, given LinkedIn removes detected misinformation and fake accounts from our platform) or LinkedIn does not have a reasonable means to compute the requested metrics.											
	SLI 14.2.1		SLI 14.2.2				SLI 14.2.3			SLI 14.2.4		
	Nr of instances of identified TTPs The number of fake accounts reported in TTP 1 SLI 14.2.1 that engaged with a feed post between 1 July – 31 December 2024	Nr of actions taken by type	Views/ impressions/ before action	Interaction/ engagement before action	Views/ impressions/ after action	Interaction/ engagement after action	Penetration and impact on genuine users	Trends on targeted audiences	Trends on narratives used	TTPs related content in relation to overall content on the service	Views/ impressions of TTP related content (in relation to overall views/impressions on the service)	Interaction/ engagement with TTP related content (in relation to overall interaction/engagement on the service)
Member States												
Austria	1,148											
Belgium	1,399											
Bulgaria	791											
Croatia	373											
Cyprus	312											
Czech Republic	740											
Denmark	648											
Estonia	166											

Finland	744											
France	14,984											
Germany	15,410											
Greece	1,230											
Hungary	475											
Ireland	1,064											
Italy	6,200											
Latvia	312											
Lithuania	678											
Luxembourg	261											
Malta	122											
Netherlands	4,451											
Poland	4,104											
Portugal	1,660											
Romania	1,328											
Slovakia	309											
Slovenia	166											
Spain	6,420											
Sweden	1,378											
Iceland	49											
Liechtenstein	4											
Norway	583											
Total EU	66,909											
Total EEA	67,545											

TTP 3	The table below addresses TTP 3: "Use of fake followers or subscribers." The table reports the number of fake accounts reported in TTP 1 SLI 14.2.1 that followed a LinkedIn profile or page between 1 July – 31 December 2024.
--------------	---

	<p>The numbers of fake accounts reported below are a subset of the fake accounts reported in TTP 1 SLI 14.2.1 that followed a LinkedIn profile or page between 1 July – 31 December 2024. For example, of the 194,153 fake accounts that LinkedIn prevented from being created or restricted between 1 July – 31 December 2024 in Austria (as reported in TTP 1 SLI 14.2.1), 9,198 of those accounts followed a LinkedIn profile or page between 1 July – 31 December 2024 (as reported below).</p> <p>Please note that the metrics provided below are total numbers and do not imply that these fake accounts were engaging in posting misinformation or disinformation.</p> <p>We have not reported metrics associated with this TTP where, for example, there is no meaningful metric to report (e.g., metrics for after the TTP in question, given LinkedIn removes detected misinformation and fake accounts from our platform) or LinkedIn does not have a reasonable means to compute the requested metrics.</p>											
	SLI 14.2.1		SLI 14.2.2				SLI 14.2.3			SLI 14.2.4		
	Nr of instances of identified TTPs The number of fake accounts reported in TTP 1 SLI 14.2.1 that followed a LinkedIn profile or page between 1 July – 31 December 2024	Nr of actions taken by type	Views/impressions before action	Interaction / engagement before action	Views/impressions after action	Interaction / engagement after action	Penetration and impact on genuine users	Trends on targeted audiences	Trends on narratives used	TTPs related content in relation to overall content on the service	Views/impressions of TTP related content (in relation to overall views/impressions on the service)	Interaction / engagement with TTP related content (in relation to overall interaction / engagement on the service)
Member States												

Austria	9,198											
Belgium	10,504											
Bulgaria	5,564											
Croatia	3,539											
Cyprus	1,631											
Czech Republic	11,763											
Denmark	6,065											
Estonia	2,523											
Finland	5,352											
France	137,403											
Germany	142,964											
Greece	11,514											
Hungary	4,856											
Ireland	11,910											
Italy	84,608											
Latvia	2,667											
Lithuania	4,464											
Luxembourg	1,567											
Malta	851											
Netherlands	39,036											
Poland	55,905											
Portugal	12,295											
Romania	10,745											
Slovakia	3,110											
Slovenia	1,298											
Spain	65,638											
Sweden	11,253											
Iceland	390											

Liechtenstein	52											
Norway	3,859											
Total EU	658,223											
Total EEA	662,524											

TTP 4	<p>The table below addresses TTP 4: “Creation of inauthentic pages, groups, chat groups, I, or domains.” SLI 14.2.1 reports the number of LinkedIn pages or groups that the fake accounts reported in TTP 1 SLI 14.2.1 created between 1 July – 31 December 2024.</p> <p>The numbers of LinkedIn pages or groups created reported below are based on the population of fake accounts reported in TTP 1 SLI 14.2.1. For example, the 194,153 fake accounts that LinkedIn prevented from being created or restricted between 1 July – 31 December 2024 in Austria (as reported in TTP 1 SLI 14.2.1) created 33 LinkedIn pages or groups between 1 July – 31 December 2024 (as reported below).</p> <p>SLI 14.2.2 reports the number of accounts in the EEA that joined or followed the pages or groups reported in TTP 4 SLI 14.2.1 between 1 July – 31 December 2024. For example, the 33 pages and groups reported for Austria in TTP4 SLI 14.2.1 had a total of 107 EEA accounts join or follow between 1 July – 31 December 2024. Whether an account qualifies as an EEA account is based on the IP address used during registration of the account.</p> <p>Please note that the metrics provided below are total numbers and do not imply that these fake accounts were engaging in posting misinformation or disinformation.</p> <p>We have not reported metrics associated with this TTP where, for example, there is no meaningful metric to report (e.g., metrics for after the TTP in question, given LinkedIn removes detected misinformation and fake accounts from our platform) or LinkedIn does not have a reasonable means to compute the requested metrics.</p>											
	SLI 14.2.1		SLI 14.2.2				SLI 14.2.3			SLI 14.2.4		
	Nr of instances of identified TTPs	Nr of actions taken by type	Views/ impressions before action	Interaction/ engagement before action	Views/ impressions after action	Interaction/ engagement after action	Penetration and impact on genuine users	Trends on targeted audiences	Trends on narratives used	TTPs related content in relation to overall	Views/ impressions of TTP related content (in relation to overall views/impressions on the service)	Interaction/ engagement with TTP related content (in relation to

	pages or groups created between 1 July – 31 December 2024 by the fake accounts reported in TTP 1 SLI 14.2.1.		or followed the pages and groups reported in TTP 4 SLI 14.2.1 between 1 July – 31 December 2024							content on the service		overall interaction /engagement on the service)
Member States												
Austria	33		107									
Belgium	35		177									
Bulgaria	18		31									
Croatia	12		78									
Cyprus	16		23									
Czech Republic	50		50									
Denmark	8		42									
Estonia	7		14									
Finland	10		35									
France	321		2,484									
Germany	195		792									
Greece	21		211									
Hungary	12		114									
Ireland	26		47									
Italy	141		2,225									
Latvia	13		35									

Lithuania	10		50									
Luxembourg	3		21									
Malta	6		35									
Netherlands	94		420									
Poland	104		349									
Portugal	79		884									
Romania	38		161									
Slovakia	20		33									
Slovenia	6		18									
Spain	191		1,499									
Sweden	28		147									
Iceland	0		5									
Liechtenstein	0		2									
Norway	9		24									
Total EU	1,497		10,082									
Total EEA	1,506		10,113									

TTP 5	LinkedIn notes that per the Integrity of Services Sub-Group, SLI 14.2.1 is theoretically fit for purpose, SLI 14.2.2 is not fit for purpose, SLI 14.2.3 is Optional/Alternative and SLI 14.2.4 is Partially fit for purpose. However, LinkedIn has not reported metrics associated with this TTP 5 (Account hijacking or impersonation) for the reasons explained in our response to QRE 14.2.1.
--------------	--

TTP 6	LinkedIn notes that per the Integrity of Services Sub-Group, SLI 14.2.1 is theoretically fit for purpose, SLI 14.2.2 is not fit for purpose, SLI 14.2.3 is Optional/Alternative and SLI 14.2.4 is Partially fit for purpose. However, LinkedIn has not reported metrics associated with this TTP 6 (Deliberately targeting vulnerable recipients (e.g. via personalized advertising, location spoofing or obfuscation)) for the reasons explained in our response to QRE 14.2.1.
--------------	--

TTP 7	LinkedIn notes that per the Integrity of Services Sub-Group, SLI 14.2.1, SLI 14.2.2 and SLI 14.2.4 are theoretically fit for purpose and SLI 14.2.3 is Optional/Alternative. However, LinkedIn has not reported metrics associated with this TTP 7 (Deploy deceptive manipulated media ("deep fakes", "cheap fakes"...)) for the reasons explained in our response to QRE 14.2.1.
--------------	---

TTP 8	LinkedIn notes that per the Integrity of Services Sub-Group, SLI 14.2.1 is theoretically fit for purpose, SLI 14.2.2 is Not fit for purpose, SLI 14.2.3 is Optional/Alternative and SLI 14.2.4 is Partially fit for purpose. However, LinkedIn has not reported metrics associated with this TTP 8 (Use “hack and leak” operation (which may or may not include doctored content)) for the reasons explained in our response to QRE 14.2.1
TTP 9	LinkedIn notes that per the Integrity of Services Sub-Group, SLI 14.2.1 is theoretically fit for purpose, SLI 14.2.2 is not fit for purpose, SLI 14.2.3 is Optional/Alternative and SLI 14.2.4 is Partially fit for purpose. However, LinkedIn has not reported metrics associated with this TTP 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)) for the reasons explained in our response to QRE 14.2.1.
TTP 10	LinkedIn notes that per the Integrity of Services Sub-Group, SLI 14.2.1 is theoretically fit for purpose, SLI 14.2.2 is not fit for purpose, SLI 14.2.3 is Optional/Alternative and SLI 14.2.4 is Partially fit for purpose. However, LinkedIn has not reported metrics associated with this TTP 10 (Use of deceptive practices to deceive/manipulate platforms algorithms, such as to create, amplify or hijack hashtags, data voids, filter bubbles, or echo chambers) for the reasons explained in our response to QRE 14.2.1.
TTP 11	LinkedIn notes that per the Integrity of Services Sub-Group, SLI 14.2.1, SLI 14.2.2 and SLI 14.2.4 are Theoretically fit for purpose, and SLI 14.2.3 is Optional/Alternative. However, LinkedIn has not reported metrics associated with this TTP 11 (Non-transparent compensated messages or promotions by influencers) for the reasons explained in our response to QRE 14.2.1. LinkedIn also notes that where members share content in an exchange for value (including monetary payment, endorsements, free products or services, or other benefit), they must label the post as a brand partnership and comply with our Advertising Policies and applicable local laws. This Help Center article provides details on how to label a post as a brand partnership.
TTP 12	LinkedIn notes that per the Integrity of Services Sub-Group, SLI 14.2.1 is Theoretically fit for purpose, SLI 14.2.2 is not fit for purpose, SLI 14.2.3 is Optional/Alternative and SLI 14.2.4 is Partially fit for purpose. However, LinkedIn has not reported metrics associated with this TTP 12 (Coordinated mass reporting of non-violative opposing content or accounts) for the reasons explained in our response to QRE 14.2.1.

Bing Search		
SLI 14.2.1 – SLI 14.2.4		
TTP 10	<p>This Section addresses TTP No. 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”), which is the TTP primarily applicable to Bing Search (including Bing generative search experiences).</p> <p>SLI 14.1.2: In response to this SLI, Bing Search is providing data on defensive search interventions employed to counteract threats and TTPs on the Bing platform. This response includes the following data categories:</p> <ul style="list-style-type: none"> • “New DSI” reflects the net new number of queries treated with defensive search interventions during the Reporting Period (across all of Bing) since the preceding reporting period. Although Member State reporting is requested, because Bing Search takes defensive search actions globally (rather than on a per country basis), each defensive search action would necessarily be implemented in an EU member state, and it is not feasible to provide Member State reporting for globally actioned measures. See SLI 14.2.2 for more detailed Member State reporting. • “AutoSuggest DSI” reflects the number of search query suggestions that were suppressed for queries entered by users in the EEA (including traditional web search and Copilot in Bing) during the Reporting Period. <p>SLI 14.2.2: Bing cannot provide data on interaction or engagement, as Bing does not allow users to “like” or “share” content within Bing and this SLI metric appears oriented to social or sharing platforms. Bing also cannot provide “before and after” data due to the preventative nature of search interventions and query-driven nature of web search. Nonetheless, below Bing Search has provided user impressions for queries that were treated with “defensive search” interventions across all of Bing Search during the Reporting Period.</p> <ul style="list-style-type: none"> • “Unique Queries DSI” reflects the total number of unique queries searched by users in the EEA that were treated with defensive search interventions during the Reporting Period. • “DSI Query Impressions” reflects the number of impressions for unique queries treated with defensive search interventions that appeared to users in the EEA during the Reporting Period. <p>SLI 14.2.3 – This SLI is not applicable to search engines, as Bing Search is not an online platform that allows for user hosted content or public sharing of user generated content with other users. User accounts in the manner contemplated under this provision are not available in search (i.e. registered user accounts are not capable of amplifying creating or amplifying content as one may through a social media network).</p> <p>For SLI 14.2.4 – This SLI is also not applicable to search engines for the above reasons.</p>	
	SLI 14.2.1	SLI 14.2.2

	Nr of actions taken by type	Nr of actions taken by type			Interaction/ engagement before action
	New DSI	Autosuggest DSI	Unique Queries DSI	DSI Query Impressions	N/A
Member States					
Austria		1,163,867	16,147	239,285	
Belgium		1,997,745	23,562	362,660	
Bulgaria		1,475	34	60	
Croatia		335	13	19	
Cyprus		203	11	14	
Czech Republic		3,658	64	110	
Denmark		672,541	1,114	138,488	
Estonia		231	17	20	
Finland		498,591	8,610	235,038	
France		8,892,324	59,006	2,396,725	
Germany		12,369,375	82,990	2,972,910	
Greece		1,158	17	25	
Hungary		3,249	31	52	
Ireland		506,151	26,277	246,692	
Italy		4,268,446	30,466	828,014	
Latvia		484	28	46	
Lithuania		397	18	24	
Luxembourg		90	3	10	
Malta		119	13	13	
Netherlands		3,242,718	35,638	498,064	
Poland		2,606,075	28,271	684,654	
Portugal		739,093	19,505	263,932	
Romania		2,755	63	143	
Slovakia		874	27	29	
Slovenia		228	6	7	

Spain		3,732,912	33,959	1,094,565	
Sweden		1,508,028	27,583	377,152	
Iceland		28	24	38	
Liechtenstein		0	1	1	
Norway		1,473,136	18,699	202,148	
Total EU		42,213,122	220,880	10,540,938	
Total EEA		43,686,286	239,604	10,743,125	
Total Global	11.4 million	-	-	-	

Measure 14.3	LinkedIn	Bing Search
QRE 14.3.1	<p>The relevant Taskforce Subgroup has considered the list of TTPs adopted in the second half of 2022 (and reported on in Microsoft's previous reports) as being fit for purpose for the current reporting cycle. LinkedIn reiterates the need for flexibility amongst different types of services to address TTPs that are most relevant to their platforms.</p> <p>This list can be consulted below:</p> <p>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:</p> <ul style="list-style-type: none"> 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 <p>The following TTPs pertain to the dissemination of content created in the context of a disinformation campaign, which may or may not include some</p>	<p>The relevant Taskforce Subgroup has considered the list of TTPs adopted in the second half of 2022 (and reported on in Microsoft's previous reports) as being fit for purpose for the current reporting cycle. The list can be consulted below.</p> <p>However, as noted in QRE 14.1.1 and 14.1.2, many of these TTPs are inapplicable to or irrelevant to search engines. Bing reiterates the need for flexibility amongst different types of services signatories to address TTPs that are most relevant to their platforms.</p> <p>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:</p> <ul style="list-style-type: none"> 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 <p>The following TTPs pertain to the dissemination of content created in the context of a disinformation campaign, which may or may not include some</p>

	<p>forms of targeting or attempting to silence opposing views. Relevant TTPs include:</p> <ul style="list-style-type: none"> • 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 <p>Further, as noted above, the relevant Taskforce Subgroup has considered whether the SLIs for each of these TTPs are fit for purpose and classified each SLI as either Theoretically fit for purpose, Not fit for purpose, Partially fit for purpose or Optional /Alternative.</p>	<p>forms of targeting or attempting to silence opposing views. Relevant TTPs include:</p> <ul style="list-style-type: none"> • 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
--	---	--

IV. Integrity of Services

Commitment 15

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

	C.15	M 15.1	M 15.2
We signed up to the following measures of this commitment:	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search

	LinkedIn	Bing Search
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes	No
If yes, list these implementation measures here [short bullet points].	New Implementation Measures Additional transparency on use of personal data for generative AI.	New Implementation Measures Not applicable
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures LinkedIn will continue to assess its policies and services and to update them as warranted.	Planned Implementation Measures Bing consistently reviews and evaluates its policies and practices related to existing and new Bing features and adjusts as needed. Bing will continue to invest in its Responsible AI program.

Measure 15.1	LinkedIn	Bing Search
QRE 15.1.1	<p>During the reporting period, LinkedIn continued to support and launch products and features that disseminate, and enable LinkedIn members to disseminate, AI-generated textual content. LinkedIn also continues to integrate generative AI-powered features into existing products. To mitigate the potential safety risks posed by such features, LinkedIn has in place and continues to augment policies and procedures to ensure that our AI systems, including any new features are consistent with LinkedIn's Responsible AI Principles and applicable law.</p> <ol style="list-style-type: none"> 1. Privacy and Security – LinkedIn has an existing process for assessing the privacy and security of new products and initiatives, which has been augmented to recognize particular risks arising from the use of generative AI. With respect to generative AI, additional considerations include being thoughtful about the personal data used in prompt engineering and ensuring that members maintain full control of their profiles. 2. Safety – LinkedIn has an existing process for assessing the safety of new products and initiatives, that has been augmented to recognize particular risks with generative AI. New features are carefully ramped to members and rate limits are introduced to reduce the likelihood of abuse. Limiting access allows us to watch for issues that may arise. We aim to proactively identify how prompts could be misused to then mitigate potential abuse. We engage in proactive content moderation (all AI generated content is held to the same professional bar as other content on the LinkedIn platform), through applying content moderation filters to both the member inputs for prompts and the output. We also engage in reactive content moderation, through provision of member tools to report policy-violating issues with the content. Additional features have been added to 	<p>Microsoft takes its commitment to responsible AI seriously and has a robust Responsible AI program. In addition to the safeguards noted earlier in this report, and discussed thoroughly at How Bing Delivers Search Results, Microsoft has implemented a number of measures and policies to help counter attempts to manipulate AI systems that generate content.</p> <p>Bing's generative AI experiences were developed in accordance with Microsoft's AI Principles, Microsoft's Responsible AI Standard, and in partnership with responsible AI experts across the company, including Microsoft's Office of Responsible AI, engineering teams, Microsoft Research, and the AI Ethics and Effects in Engineering and Research (AETHER) committee. All Microsoft processes, programs, or tools utilizing AI, including Bing's generative AI experiences, must adhere to Microsoft's Responsible AI Standard and undertake impact assessments to help ensure responsible use of AI-influenced algorithms and processes for any new product features. More details on Microsoft's Responsible AI Standard, impact assessments, and resources on Responsible AI are located at Microsoft's Responsible AI Hub. Bing also conducts detailed annual risk assessments that evaluate risks posed by its systems (including generative AI features) and evaluates current and potential risk mitigation measures.</p> <p>In addition to the measures discussed at QREs 14.1.1 and 14.1.2 (including pre and post launch testing, the use of classifiers and metaprompting, defensive search interventions, reporting functionality, and increased operations and incident response), Microsoft has incorporated the following safeguards and policies for countering prohibited manipulative practices for AI systems.</p> <p>To help facilitate safe use of Bing's generative AI experiences, Microsoft published Copilot AI Experiences Terms (applicable to Copilot in Bing through its retirement in October 2024) and Bing's Image Creator Terms of</p>

	<p>these tools that address generative AI-specific issues such as ‘hallucinations.’ Additionally, all generative AI-powered features that have outputs that are directly visible to LinkedIn users, go through (1) manual and automated “red teaming,” to test the generative AI-powered feature and to identify and mitigate any vulnerabilities, and (2) quality assurance assessments on response quality, accuracy, and hallucinations with the goal to remediate discovered inaccuracies.</p> <p>3. Fairness and Inclusion – LinkedIn has a cross functional team that designs policy and process to proactively mitigate the risk that AI tools, including generative AI tools, perpetuate societal biases or facilitate discrimination. To promote fairness and inclusion, we target two key areas - content subject and communities. With respect to content subjects, prompts are engineered to reduce the risk of biased content, blocklists are leveraged to replace harmful terms with neutral terms, and member feedback is monitored to learn and improve. With respect to communities, in addition to a focus on problematic content like stereotypes, we are working to expand the member communities that are served by our generative AI tools. Additionally, LinkedIn continues to invest in methodologies and techniques to more broadly ensure algorithmic fairness.</p> <p>4. Transparency – LinkedIn is committed to being transparent with members. With respect to generative AI products and features, our goal is to educate members about the technology and our use of it such that they can make their own decisions about how to engage with it. For example, with Collaborative Articles we identify the use of AI in the relevant UI and we provide additional detail in a linked Help Center article. Additionally, LinkedIn labels content containing industry-leading “Content Credentials” technology developed by the Coalition for Content</p>	<p>Use (including a user Code of Conduct) and implemented other mechanisms to help prevent and address misuse of these features. The Supplemental Terms prohibit users from “engaging in activity that is fraudulent, false, or misleading” and “attempting to create or share content that could mislead or deceive others, including for example creation of disinformation, content enabling fraud, or deceptive impersonation.” Users that violate these terms may be suspended from the service. In addition, Bing’s generative AI experiences may block certain text prompts that violate or are likely to violate the Code of Conduct. Repeated attempts to produce prohibited content or other violations of the Code of Conduct may result in service or account suspension. In addition,</p> <p>Microsoft maintains social listening pipelines where insights and user feedback (including efforts to “jailbreak” generative AI experiences) are collected from the open Internet. These insights and user feedback are manually reviewed by humans, analyzed daily, and shared across the Bing product teams and with product leadership to identify new areas of concern and implement additional mitigations as needed. Microsoft also has set up a robust user reporting and appeal process to review and respond to user concerns of harmful or misleading content.</p> <p>Bing’s generative AI experiences also provide several touchpoints for meaningful AI disclosures, where users are notified that they are interacting with an AI system and are presented with opportunities to learn more about these features and generative AI, such as through in-product disclaimers, as discussed in How Bing Delivers Search Results educational FAQs, and blog posts. Empowering users with this knowledge can help them avoid over-relying on AI and learn about the system’s strengths and limitations.</p> <p>In addition to the measures discussed above, Microsoft has worked to deliver an experience that encourages responsible use of Bing’s generative AI features and to limit the generation of harmful or unsafe images. When</p>
--	---	--

	<p>Provenance and Authenticity (“C2PA”), including AI-generated content containing C2PA metadata. Content Credentials on LinkedIn show as a “Cr” icon on images and videos that contain C2PA metadata, particularly on highly visible surfaces such as the feed. By clicking the icon, LinkedIn members can trace the origin of the AI-created media, including the source and history of the content, and whether it was created or edited by AI. Additionally, LinkedIn provides members with information on how their personal data is used for generative AI in the LinkedIn Help Center, including how personal data is used for content generating AI model training. As of December 31, 2024, LinkedIn did not train content generating AI models on data from members located in the EU, EEA, UK, Switzerland, Canada, Hong Kong, or mainland China.</p> <p>5. Accountability – In addition to the privacy, security, and safety processes discussed above, for AI tools we have additional assessments of training data and model cards so we can more appropriately assess risks and develop mitigations for the AI models that support our AI products and initiatives.</p>	<p>these systems detect that a potentially harmful image could be generated by a prompt, it blocks the prompt and warns the user.</p> <p>Microsoft’s Responsible AI systems will continue to improve, and Microsoft regularly incorporates user and third-party feedback reported via Bing and Copilot Feedback buttons and its user reporting tools.</p> <p>See also QRE 20.1.1.</p>
Measure 15.2	LinkedIn	Bing Search
QRE 15.2.1	<p>With respect to the algorithms used for detection, moderation, and sanctioning of impermissible conduct and content, please see:</p> <ul style="list-style-type: none"> • QRE 15.1.1 (policies for countering prohibited manipulative practices in AI systems); • QRE 18.1.3 (design of recommender systems and related AI); • QRE 18.2.1 (policies and procedures to limit spread of harmful false or misleading information); • QRE 22.2.1 (actions taken to assist members in identifying trustworthy content); and • QRE 23.2.1 (actions taken to ensure integrity of reporting and appeals process). 	<p>As a search engine, Bing Search operates differently from social media websites and other online platforms that host content. Bing Search does not host user-generated content and does not use algorithms to detect, moderate or sanction user-provided content except for limited circumstances outside the scope of this Code of Practice (e.g., the use of PhotoDNA software to detect and report child sexually explicit imagery uploaded to visual search). As to third party websites indexed by Bing Search, Bing Search does not use algorithms to detect, monitor or sanction such websites, except for limited circumstances outside the scope of this Code of Practice (e.g., the use of PhotoDNA software to detect and report child sexually explicit imagery). Bing users have many legitimate reasons for seeking out content in search that may be harmful or offensive in other</p>

		<p>contexts, and so Bing Search works to provide as comprehensive and useful of a collection of results as possible and does not proactively intervene to limit access to legal content. In some limited cases Bing Search may take action to remove or limit access to third party links where quality, safety, user demand, relevant laws, and/or public policy concerns exist, but these interventions are reactive; Bing generally does not engage in proactive algorithmic interventions to remove content.</p> <p>Bing's generative AI features include additional enhanced safety features such as classifiers, filters, and a bespoke metaprompt that further limits the likelihood of harmful content appearing in generative AI features. Microsoft has engaged in extensive Responsible AI reviews regarding generative AI features in order to ensure outputs are not biased or discriminatory. It has also implemented additional filtering and classifiers to prevent generative AI experiences from returning what Bing considers "low authority" content as part of an answer and to help address impermissible content and behaviors. Microsoft is also continually working to ensure that its generative features do not over-block outputs so that users are able to access the information they seek and measures and monitors conversation metrics to improve the interventions to balance the harm prevention and provide users with useful information.</p> <p>Lastly, Microsoft has endeavored to provide transparency about how it designed and tested its generative AI features with responsible AI in mind via blog posts, FAQs, presentations, and responsible AI documentation, for example How Bing Delivers Search Results. In May 2024, Microsoft also released its first ever Responsible AI Transparency Report, which provides additional detail on Microsoft's Responsible AI programs, including insights into how Microsoft builds applications that use generative AI and makes decisions and oversees the deployment of those applications, among other things.</p>
--	--	--

IV. Integrity of Services

Commitment 16

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

	C.16	M 16.1	M 16.2
We signed up to the following measures of this commitment:	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn

	LinkedIn	Bing Search
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	Yes
If yes, list these implementation measures here [short bullet points].	<p>New Implementation Measures</p> <p>Not applicable</p>	<p>New Implementation Measures</p> <p>Throughout the reporting period Microsoft continued to publish threat intelligence related to foreign cyber enabled interference in elections around the world. This intelligence was shared publicly so election authorities around the world, including in Romania and Croatia could benefit from the insights into foreign adversary activity.</p> <p>Bing participated in the Elections Working Group and established additional intake channels to</p>

		facilitate cross-platform information sharing in relation to the French, Romanian and Croatian Elections.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	<p>Planned Implementation Measures</p> <p>We look forward to continuing to work on this commitment with the other signatories as we develop further cross platform information sharing.</p>	<p>Planned Implementation Measures</p> <p>We look forward to continuing to work on this commitment with the other signatories as we develop further cross platform information sharing.</p>

Measure 16.1	LinkedIn	Bing Search
QRE 16.1.1	<p>LinkedIn, through Microsoft, is an active participant in and contributor to the Task-force's Crisis Response subgroup, in which it proactively provides analysis and data, related to influence operations, foreign interference in information space and relevant incidents that emerges on its service. Microsoft's internal threat detection and research teams, including Microsoft Threat Analysis Center (MTAC), Microsoft Threat Intelligence Center (MSTIC), Microsoft Research (MSR), and AI For Good, collect and analyse data on actors of disinformation, misinformation and information manipulation across platforms.</p> <p>Moreover, LinkedIn works with numerous partners to facilitate the flow of information to tackle purveyors of disinformation, including disinformation spread by state-sponsored and institutional actors.</p>	<p>Bing Search, through Microsoft, is an active participant in and contributor to the Task-force's Crisis Response subgroup, in which it proactively provides analysis and data related to influence operations, foreign interference in information space and relevant incidents that emerges on its service.</p> <p>Microsoft's internal threat detection and research teams, including Microsoft Threat Analysis Center (MTAC), Microsoft Threat Intelligence Center (MSTIC), Microsoft Research (MSR), and AI For Good, collect and analyse data on actors of disinformation, misinformation and information manipulation across platforms. These teams work with external organisations and companies to share and ingest data that help support Microsoft product and service teams effectively respond to issues and threats.</p>

	<p>LinkedIn maintains an internal Trust and Safety team composed of threat investigators and intelligence analysts to address disinformation. This team works with peers and other stakeholders, including our Artificial Intelligence modelling team, to identify and remove nation-state actors and coordinated inauthentic campaigns. LinkedIn conducts investigations into election-related influence operations and nation-state targeting including continued information sharing on threats with industry peers and Law Enforcement on a regular basis. LinkedIn works with peer companies and other stakeholders to receive and share indicators related to fake accounts created by state-sponsored actors, such as confirmed Tactics, Techniques, and Protocols (TTPs) and Indicators of Compromise (IOC). This exchange of information leads to a better understanding of the incentives of sophisticated and well-funded threat actors and how they evolve their TTPs to achieve those goals, which assists LinkedIn in their identification and removal. Any associated disinformation content is verified by our internal or external fact-checkers as needed, and coordinated inauthentic behaviours (CIBs) are also removed by our Threat Prevention and Defense team.</p> <p>LinkedIn, along with its parent company, Microsoft, is heavily involved in threat exchanges. These threat exchanges take various forms, such as: 1) regular discussion amongst industry peers to discuss high-level trends and campaigns; and, 2) one-on-one engagement with individual peer companies to discuss TTPs and IOCs. This exchange of information leads to a better understanding of the incentives of sophisticated and well-funded threat actors and how they evolve their TTPs to achieve those goals, which assists us in their identification and removal.</p> <p>LinkedIn always stands ready to receive and investigate any leads we receive from peers and other external stakeholders. In addition to one-on-one engagement with peers, we also consume intelligence from vendors and investigate any TTPs and IOCs made available in peer</p>	<p>Microsoft also works to identify and track nation-state information operations targeting democracies across the world and works with trusted third-party partners for early indicators of narratives, hashtags, or information operations that can be leveraged to inform early detection and defensive search strategies for Bing. Through Microsoft's Democracy Forward team and MTAC, Microsoft also offers mediums for election authorities, including in the EEA member states, to have lines of communication with Microsoft to identify possible foreign information operations targeting elections.</p> <p>See also QRE 14.1.2.</p>
--	---	--

	disclosures. In turn, we also regularly release information about policy-violating content on our platform in publicly-available transparency reports and blog posts.					
SLI 16.1.1 – Numbers of actions as a result of information sharing	We look forward to providing reports where appropriate in future reporting periods.			See SLI 14.2.1 for defensive search interventions data, which is based in part on information and threat intelligence gathered through information sharing with third parties, as well as the internal Microsoft and Bing resources noted in QREs 16.1.1 and 14.2.1. Given the multipronged approach Microsoft and Bing take to monitoring and actioning influence operations and sources of misinformation and disinformation and the multiple internal and external sources relied upon, it is challenging to provide precise reporting on whether an incidence of single information sharing results in a corresponding defensive search intervention or other action.		
	Nr of actions taken (total)	Type of detected content	Other relevant metrics	Nr of actions taken (total)	Type of detected content	Other relevant metrics
Measure 16.2	LinkedIn			Bing Search		
QRE 16.2.1	We look forward to working on this commitment with the other signatories as we develop further cross-platform information sharing.			We look forward to working on this commitment with the other signatories as we develop further cross-platform information sharing and best practices for measuring such information consistently.		

V. Empowering Users

Commitments 17 - 25

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.

	C.17	M 17.1	M 17.2	M 17.3
We signed up to the following measures of this commitment:	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search

	LinkedIn	Bing Search
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	No
If yes, list these implementation measures here [short bullet points].	New Implementation Measures Not applicable	New Implementation Measures Not applicable
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No	No
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures Not applicable.	Planned Implementation Measures Bing Search regularly reviews and evaluates its user tools, policies, and practices and adjusts and updates policies as needed. While Bing's existing programs are already designed to address these issues, Bing regularly evaluates its measures

		and endeavors to improve and work to respond quickly to new threats or issues as they arise.
--	--	--

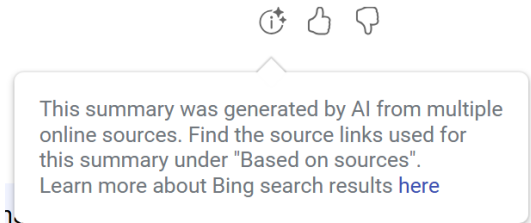
Measure 17.1	LinkedIn	Bing Search
QRE 17.1.1	<p>As the world around us changes, LinkedIn continues to evolve and adapt our systems and practices for combating misinformation and other inauthentic behaviour on our platform, including to respond to the unique challenges presented by world events.</p> <p>LinkedIn's <u>Professional Community Policies</u>, which all members agree to abide by on joining LinkedIn, prohibit misinformation. As described in more detail in our response to QRE 18.1.1, LinkedIn uses a combination of automated and manual activity to keep content that violates our policies off of LinkedIn.</p> <p>LinkedIn also aims to educate its members about civic discourse, electoral processes, and public security through its global team of news editors. These editors provide trustworthy and authoritative content to LinkedIn's member-base, and its content moderation teams closely monitor associated platform conversations in a number of languages.</p> <p>In addition to broader measures, LinkedIn has taken special care to counter low authority information in relation to the war of aggression by Russia on Ukraine, the Israel-Hamas Conflict, and the European Elections, as detailed in relevant chapters.</p> <p>For example, during pre-election cycles, LinkedIn relies on trusted and reputable publisher sources for featured shares, focusing on the</p>	<p>Bing Search offers a number of tools to help users understand the context and trustworthiness of search results. Even in circumstances where a user is expressly seeking low authority content (or if there is a data void so little to no high authority content exists for a query), Bing Search provides tools to users that can help improve their digital literacy and avoid harms resulting from engaging with misleading or inaccurate content. For example, Bing Search may include answers or public service announcements at the top of search results pointing users to high authority information on a searched topic such as key global elections or warnings on particular URLs known to contain harmful information (such as unaccredited online pharmacies and sites containing malware).</p> <p>Where circumstances warrant (such as public health crises or major elections), Bing Search may provide information hubs for users to easily access a centralized repository of high authority information.</p> <p>Bing Search also provides users with informative panels and direct answers to certain search queries and is now available in a multitude of global languages. Bing Search's "Knowledge Cards" feature also gives users a single view of authoritative information on a specific topic. An example is shown below.</p>

<p>policy impact on businesses and professionals around the EU. LinkedIn also curates links to topical landing pages from trusted publishers to provide members with easy and reliable entry points to more detailed coverage. LinkedIn does not compete with trusted publishers for speed or depth of coverage, but instead aims to connect their existing coverage to LinkedIn members and their needs. During important events in European Elections, this team provides manually curated and localised storylines.</p> <p>We also work to identify and remove misinformation and inauthentic behaviour from our platform. As we continue to improve, we are committed to helping our members make informed decisions about content they find on LinkedIn, so we work with Microsoft to provide tools that assist our members in identifying trustworthy, relevant, authentic, and diverse content.</p> <p>LinkedIn's Professional Community Policies clearly detail the objectionable and harmful content that is not allowed on LinkedIn. Misinformation and inauthentic content is not allowed, and our automated defenses take proactive steps to remove them. LinkedIn's blog provides information regarding our efforts, including How We're Protecting Members From Fake Profiles, Automated Fake Account Detection, and An Update on How We Keep Members Safe.</p> <p>LinkedIn members can report content that violates our Professional Community Policies, including misinformation and inauthentic content. Our Trust and Safety teams work every day to identify and restrict such activity, and if reported content violates the Professional Community Policies, it will be actioned in accordance with our policies.</p> <p>LinkedIn members can identify misinformation and inauthentic behaviour by utilising the News Literacy Project, The Trust Project</p>	 <p>Bing Search provides users with public service announcements (PSAs). PSAs are user messages that appear as answer boxes at the top of a list of search results for certain triggering queries, providing information on potential risks associated with that query and/or pointing to support resources. PSAs are triggered by queries on specific topics, such as child pornography, attempts to purchase illegal pharmaceuticals, suicide, etc.</p> <p>Bing search also partners with trusted election authorities to empower voters with authoritative election information on Bing. Bing leverages partnerships with EU election authorities to help direct users to trusted and/or official sources of information concerning elections and voting information.</p> <p>For example, Bing launched specialized How to Vote Answers in advance of the French snap elections held June-July 2024. Examples of how these special answers appear to users are shown below.</p>
--	---

and Verified, all of which develop information literacy campaigns built on industry research and best practices. The News Literacy Project campaign developed a quiz that tests a person's ability to identify why the information they are seeing is false and inaccurate in less than five minutes. The Trust Project campaign developed the research-backed 8 Trust Indicators, which aim to improve consumers ability to identify reliable, ethical journalism. Finally, Verified delivers lifesaving information and fact-based advice to build digital literacy that helps communities protect themselves from misinformation. LinkedIn has also published an article in our Help Center compiling these useful resources on misinformation and inauthentic behaviour.



In addition to the features available for core search experiences, Bing generative features notify users that they are interacting with an AI system and are presented with opportunities to learn more about these features and generative AI, such as through in-product disclaimers. For example, Bing Generative Search results displays the below disclosure to users:

		 <p>Microsoft also offers meaningful resources for users interested in learning more about generative AI features and tools through blog posts, articles, information hubs, and support pages. In addition to teaching AI basics and how-tos, these resources reiterate the importance of checking AI-generated materials and understanding the strengths and limitations of AI. See e.g., Microsoft AI help & learning.</p> <p>As part of Microsoft's Tech Accord commitments, Microsoft has created trainings for political parties, candidates, and election officials to improve their understanding of what deepfakes are and how they can protect against their use in elections. At the time of writing, Microsoft has completed 50 separate training sessions across EEA countries reaching over 500 participants. Countries include Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Netherlands, Norway, Portugal, Slovakia, Spain, and Sweden.</p> <p>Microsoft is committed to providing resources, educational materials, and guides so that users can develop literacy when interacting with AI systems and will continue to explore ways to further educate the public on important generative AI topics.</p>
SLI 17.1.1 - actions enforcing policies above	The table below reports the number of visitors to LinkedIn's Help Center article compiling useful resources on misinformation during the period 1 July – 31 December 2024.	<p>Methodology of data measurement:</p> <p>Knowledge Cards ("KC") – Represents viewership of Knowledge Cards (of all types/topics) during the Reporting Period</p>

				<p>Transparency Hub Viewership (“TH”) – Represents the total views of the Microsoft Transparency Report Hub during the Reporting Period.</p> <p>Public Service Announcement (“PSA”) – Represents views of public service announcement panels (of all types/topics) rendered in Bing to EU users during the Reporting Period.</p>				
	Total count of the tool’s impressions	Interactions/engagement with the tool	Other relevant metrics		Interactions/engagement with the tool	Total count of the tool’s impressions	Total count of the tool’s impressions	Other relevant metrics
	Number of visits during the period 1 July – 31 December 2024				KC	TH	PSA	
Member States								
Austria	35				108,761,673	57	70,220	
Belgium	15				200,650,612	58	133,860	
Bulgaria	39				38,569,264	21	27,380	
Croatia	19				2,7201,309	8	21,260	
Cyprus	4				8,784,806	11	5,280	
Czech Republic	28				138,432,602	54	66,940	
Denmark	80				80,485,036	58	62,580	
Estonia	18				15,330,027	10	11,760	
Finland	81				86,792,314	46	49,120	
France	290				1,063,056,890	144	497,580	
Germany	794				1,108,464,294	324	604,440	
Greece	24				56,864,591	19	36,900	
Hungary	19				70,877,762	32	44,360	
Ireland	63				110,462,651	17	195,720	

Italy	3,988				686,807,990	81	183,140	
Latvia	354				17,582,909	11	223,340	
Lithuania	185				28,626,206	14	23,560	
Luxembourg	21				11,744,763	8	5,400	
Malta	10				8,206,968	0	9,080	
Netherlands	632				309,694,218	313	251,780	
Poland	166				463,903,783	112	202,920	
Portugal	32				151,513,785	26	82,700	
Romania	56				83,347,298	30	59,440	
Slovakia	15				39,365,393	21	26,460	
Slovenia	7				1,8367,447	11	13,860	
Spain	109				816,296,463	136	206,520	
Sweden	99				173,528,035	143	138,620	
Iceland	14				6,685,380	24	5,480	
Liechtenstein	1				729,055	6	200	
Norway	45				94,912,507	50	76,540	
Total EU	7,184				5,923,719,089	1,765	3,155,880	
Total EEA	7,244				6,026,046,031	1,845	3,073,660	

Measure 17.2	LinkedIn	Bing Search
QRE 17.2.1	<p>Microsoft works with leading media and information literacy partners globally to support the development and promotion of media literacy campaigns.</p> <p>Microsoft has continued its partnerships with third-party organisations, including the News Literacy Project and The Trust Project, to amplify media literacy campaigns while continuing introductory calls with new organizations to grow additional campaigns' reach to new markets.</p>	<p>Microsoft works with leading media and information literacy partners globally to support the development and promotion of media literacy campaigns that benefit users across Microsoft services and the broader ecosystem.</p> <p>Microsoft has also launched a media literacy initiative focusing on awareness about deceptive use of AI on elections and how to identify AI generated content: Combating the deceptive use of AI in elections (microsoft.com)</p>

SLI 17.2.1 - actions enforcing policies above	Beginning March 2024 and continuing through Autumn 2024, Microsoft launched a new “Be Informed, Not Misled” campaign from the News Literacy Project. This campaign averages millions of impressions monthly.				In May 2024, Microsoft, in collaboration with OpenAI, launched the Societal Resilience Grants to support various organizations in promoting AI literacy, ethical AI use, and societal resilience against AI-related challenges. The grants were awarded to the Older Adults Technology Services from AARP, International IDEA, Partnership on AI, Coalition for Content Provenance and Authenticity (C2PA), and WITNESS. These initiatives have reached national election bodies in 26 countries, 500,000 older adults, and 250 global journalists, demonstrating a comprehensive approach to addressing AI threats and fostering responsible AI practices.			
	Microsoft has also launched a media literacy initiative focusing on awareness about deceptive use of AI on elections and how to identify AI generated content: Combating the deceptive use of AI in elections.				As part of Microsoft’s Tech Accord commitments, Microsoft has created trainings for political parties, candidates, and election officials to improve their understanding of what deepfakes are and how they can protect against their use in elections. At the time of writing, Microsoft has completed 50 separate training sessions across EEA countries reaching over 500 participants. Countries include Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Netherlands, Norway, Portugal, Slovakia, Spain, and Sweden.			
	Methodology of data measurement:				Methodology of data measurement:			
	Nr of media literacy/ awareness raising activities organised/ participated in	Reach of campaigns	Nr of participants	Nr of interactions with online assets	Nr of media literacy/ awareness raising activities organised/ participated in	Reach of campaigns	Nr of participants	Nr of interactions with online assets
					50 training sessions	Countries including Austria, Belgium,	500 participants	

						Denmark, Finland, France, Germany, Greece, Ireland, Italy, Netherlands, Norway, Portugal, Slovakia, Spain, and Sweden.		
--	--	--	--	--	--	---	--	--

Measure 17.3	LinkedIn	Bing Search
QRE 17.3.1	<p>Microsoft continues to work with multiple organisations to develop and promote media literacy campaigns, including 2024 campaigns from the News Literacy Project and The Trust Project to promote information literacy resources on Microsoft platforms.</p> <p>For the next reporting period, Microsoft is continuing to work with existing and new partners to create, disseminate, and report on expanded literacy campaigns in EEA markets. Please also see response to QRE 17.1.1.</p>	<p>Microsoft continues to work with multiple organisations to develop and promote media literacy campaigns, including 2024 campaigns from the News Literacy Project and The Trust Project to promote information literacy resources on Microsoft platforms.</p> <p>Since its last report, Microsoft continues to grow partnerships to strengthen the company's capacity and ability to combat information operations globally.</p> <p>Microsoft is continuing to work with existing and new partners to create, disseminate, and report on expanded literacy campaigns in EEA markets, such as delivering additional deepfake awareness trainings. Including International IDEA is on track to deliver 5 AI and Elections Trainings between November 2024 and May 2025. These trainings will reach global election officials, civil society and journalists. The training will provide participants with an enhanced understanding of AI, its ethical implications, and its uses and benefits in electoral management. Microsoft's Deepfake content will be integrated into the curriculum.</p>

V. Empowering Users

Commitment 18

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

	C.18	M 18.1	M 18.2	M 18.3
We signed up to the following measures of this commitment:	LinkedIn Bing Search	LinkedIn	LinkedIn Bing Search	LinkedIn Bing Search

	LinkedIn	Bing Search
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	Yes
If yes, list these implementation measures here [short bullet points].	<p>New Implementation Measures</p> <p>Not applicable</p>	<p>New Implementation Measures</p> <p>Bing regularly reviews and implements mitigations, safeguards, and safe design considerations to help proactively address, prevent and mitigate harms arising from potential misuse of generative AI search experiences, including viral propagation of content, and provides updates to public facing transparency documents, such as How Bing Delivers Search Results. However, Bing features do not</p>

		allow users to post or share content within Bing so virality is not possible on the platform itself.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	<p>Planned Implementation Measures</p> <p>LinkedIn will continue to assess its policies and services and to update them as warranted.</p>	<p>Planned Implementation Measures</p> <p>Bing is regularly reviewing and evaluating its policies and practices related to features and adjusts and updates policies as needed. Bing continues to explore additional potential research opportunities and partnerships related to the spread of harmful misinformation and/or disinformation.</p>

Measure 18.1	LinkedIn	This measure is not relevant or pertinent to Bing Search as search engines do not fuel virality of disinformation via users sharing content.
QRE 18.1.1	<p>Outline relevant actions</p> <p>With respect to AI design, please see QRE 18.1.3</p> <p>With respect to additional tools, procedures, or features, please see:</p> <ul style="list-style-type: none"> • QRE 17.1.1 (editorial practices to provide members with trustworthy news); • QRE 18.2.1 (policies and procedures to limit spread of harmful false or misleading information); 	

	<ul style="list-style-type: none"> • QRE 21.1.1 (action taken when information is identified as misinformation); • QRE 22.1.1 (features and systems related to fake and inauthentic profiles); • QRE 22.2.1 (actions taken to assist members identify trustworthy content); • QRE 23.2.1 (actions taken to ensure integrity of reporting and appeals process). 	
QRE 18.1.2	<p>The main parameters of the LinkedIn feed recommender systems are as follows:</p> <ul style="list-style-type: none"> - Identity: We seek to contextualise content based on who a member is by looking at their profile, for example: Who are you? Where do you work? What are your skills? Who are your connections? Where is your profile location? - Content: We aim to match appropriate content to each member by evaluating, for example: How many times was the feed update viewed? How many times was it reacted to? What is the content about? How old is it? Is the update sharing knowledge or professional advice? Is the update from someone the member is connected to or follows? What language is it written in? Is the conversation constructive and professional? Will engagement on the update lead to future high-quality content? What companies, people, or topics are mentioned in the update? - Member Activity: Finally, we look at how a member engages with content and examine, for example: What have you reacted to and shared in the past? Who do you interact with most frequently or recently? Where do you spend the most time in your feed? Which hashtags, people or companies do you follow? Who are your connections? What types of topics are you interested in? What other members follow you? What actions have other members taken on your posts? How long has it been since the foregoing actions took place? 	

	<p>Combining these and other related signals, the LinkedIn feed recommender systems rank the content for the member, with the goal of showing the member high quality content that the member will enjoy consuming and can lead to further creation on the platform. To do this, the feed optimizes for content that a member is most likely to find highly valuable, which in turn is likely to lead the member to act on (e.g., react, comment, or reshare).</p>	
QRE 18.1.3	<p>At LinkedIn, our guiding principle is “Members First.” It ensures we honour our responsibility to <u>protect our members and maintain their trust</u> in every decision we make, and puts their interests first. A key area where we apply this value in engineering is within our design process. We call this “responsible design,” which means that everything we build is intended to work as part of a unified system that delivers the best member experience, provides the right protections for our members and customers, and mitigates any unintended consequences in our products.</p> <p>One of the core pillars of “responsible design” is “responsible AI,” which follows the <u>LinkedIn Responsible AI Principles</u>, which are inspired by and aligned with <u>Microsoft’s Responsible AI Principles</u>. The LinkedIn Responsible AI Principles are to advance economic opportunity, uphold trust, promote fairness and inclusion, provide transparency, and embrace accountability. In addition to the LinkedIn Responsible AI Principles, responsible AI is also about intent and impact. “Intent” involves evaluating training data, designing systems, and reviewing model performance before the model is ever deployed to production to make sure that our principles are reflected at every step in the process. It includes actively changing our products and algorithms to empower every member. “Impact” covers detecting and monitoring the ways that people interact with products and features after they are deployed. We do this by measuring whether they provide significant value and empower individuals to reach their goals. Intent and impact are a cyclical process of</p>	

	<p>refinement that go hand-in-hand towards the broader goal of responsible design.</p> <p>With respect to safety, we seek to keep content that violates our Professional Community Policies off of LinkedIn. This is done through a combination of automated and manual activity. Our first layer of protection is using AI to proactively filter out bad content and deliver relevant experiences for our members. We use content (like certain key words or images) that has previously been identified as violating our content policies to help inform our AI models so that we can better identify and restrict similar content from being posted in the future. The second layer of protection uses AI to flag content that is likely to be violative for human review. This occurs when the algorithm is not confident enough to warrant automatic removal. The third layer is member led, where members report content and then our team of reviewers evaluates the content and removes it if it is found to be in violation of our policies.</p> <p>Quantifying the above process to monitor how many content violations are successfully prevented is another important task that our Data Science team prioritises, such that we can continuously refine our processes to improve detection and prevention of violative content.</p> <p>Please also see:</p> <ul style="list-style-type: none"> • QRE 17.1.1 (editorial practices to provide members with trustworthy news); • QRE 18.2.1 (policies and procedures to limit spread of harmful false or misleading information); • QRE 21.1.1 (action taken when information is identified as misinformation); • QRE 22.1.1 (features and systems related to fake and inauthentic profiles); 	
--	--	--

	<ul style="list-style-type: none"> QRE 22.2.1 (actions taken to assist members identify trustworthy content); QRE 23.2.1 (actions taken to ensure integrity of reporting and appeals process). 							
SLI 18.1.1 - actions proving effectiveness of measures and policies								
	Reduction of prevalence of disinformation	Reduction of views/ impressions of disinformation	Increase in visibility of authoritative information	Other relevant metrics				

Measure 18.2	LinkedIn	Bing Search
QRE 18.2.1	<p>LinkedIn is an online professional network. On LinkedIn, the world's professionals come together to find jobs, stay informed, learn new skills, and build productive relationships. The content that our members share becomes part of their professional identity and can be seen by their boss, colleagues, and potential business partners. Accordingly, the content on LinkedIn is professional in nature.</p> <p>To help keep LinkedIn safe, trusted, and professional, our Professional Community Policies clearly detail the range of objectionable and harmful content that is not allowed on LinkedIn. Fake accounts, misinformation, and inauthentic content are not allowed, and we take active steps to remove it from our platform.</p> <p>LinkedIn removes "specific claims, presented as fact, that are demonstrably false or substantially misleading and likely to cause harm." This approach applies globally and is used for purposes of content moderation and for publicly reporting figures on misinformation. Specific examples of what might constitute misinformation can be found here in our Help Center. As part of</p>	<p>Unlike social media services, for which this Commitment appears primarily oriented, search engines do not typically cause or facilitate the viral propagation of disinformation, as they do not allow users to post or share content directly on the service. Please see How Bing delivers search results and Microsoft Bing Webmaster Guidelines for an overview of how Bing Search designs its algorithms to deliver high authority and highly relevant content while minimizing the negative impact of spam and less credible information sources. Bing Search's ranking algorithms and related policies are intended to address deceptive tactics intended to manipulate the algorithms and are discussed in more detail at QREs 14.1.1 and 14.1.2. Bing Search features such as news carousels as well as the other features and policies discussed throughout this report further help minimize the risk of viral propagation of misinformation through Bing Search.</p> <p>Bing's suggestions features offer possible search queries to users to facilitate a more efficient search experience. While search suggestions are not directly tied to virality of content, Bing Search also undertakes measures to help ensure it does not inadvertently lead users to misleading or other harmful</p>

our [User Agreement](#), our Professional Community Policies are accepted by every member when joining LinkedIn and are easily available to every member.

LinkedIn creates value and preserves trust by fostering a safe, trusted, and professional platform, while honouring members' professional expression and speech. LinkedIn enables healthy on-platform conversations by facilitating the removal of misinformation that threatens its members' safety. And when content doesn't conclusively violate LinkedIn policies, LinkedIn gives the speaker the benefit of the doubt and favours speech (i.e., leaves the content up on platform).

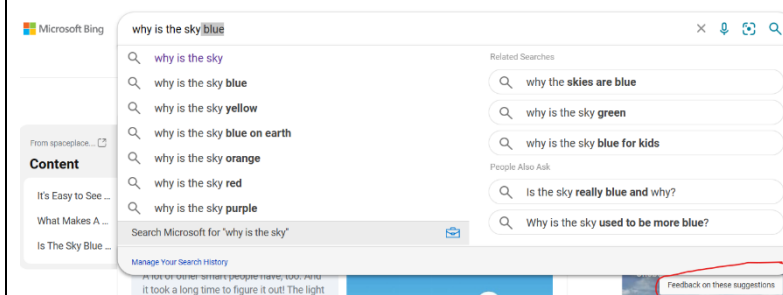
Additionally, as described in greater detail below, human review plays a significant role in our content moderation process. Additionally, Members who post content and members who report content can appeal our content moderation decisions.

Our content policies are clear and we apply them equally for all members. Within our Professional Community Policies we provide granular information and examples on what is and what is not allowed on LinkedIn.

Furthermore, LinkedIn has automated defences to identify and prevent abuse, including inauthentic behaviour, such as spam, phishing and scams, duplicate accounts, fake accounts, and misinformation. Our Trust and Safety teams work every day to identify and restrict inauthentic activity. We're regularly rolling out scalable [technologies](#) like machine learning models to keep our platform safe.

content through suggestions. Specifically, Bing Search uses a combination of proactive and reactive algorithmic and manual interventions to prevent the display of search suggestions that could lead to low authority content.

Bing Search also provides a tool for users to provide feedback on suggestions they encounter. The feedback tool is shown below.



Clicking "Feedback on these suggestions" allows users to provide specific feedback on individual suggestions on the below bases:

These suggestions are:

- ☐ Not relevant
- ☐ Not correct
- ☐ Misspelled or garbled
- ☐ Inappropriate or offensive
- ☐ Hateful to groups or individuals
- ☐ About illegal or dangerous activity
- ☐ Other

There is generally no risk of viral spread of generated content through Bing and Bing's generative AI experiences because Bing does not allow users to directly post or otherwise share content on the platform. Bing also takes steps to prevent the service from being used to create content or images that might be shared on other platforms through a multipronged approach. This

		<p>approach includes terms of use and a code of conduct, classifiers, filters, bespoke metaprompts, and robust reporting mechanisms designed to mitigate the risk of potential misuse of the platform. Supplemental Terms addressing AI powered search experiences in Bing, for example, prohibit users from using the service to generate fraudulent or misleading information, including the creation of disinformation. Bing's ranking and relevance systems for search, which are an essential component to answering user questions, work to ensure that high authority content is returned first in search results in traditional search and in chat. Where Bing's systems flag that a user's prompt or generated output may result in low authority or misleading information, the system will take steps to mitigate that possible harm through solutions, such as not returning generated content to the user, diverting the user to a different topic, or redirecting the user to traditional search. Users who encounter problematic content can report concerns via Feedback or Report a Concern tools.</p>
SLI 18.2.1 - actions taken in response to policy violations	<p>Methodology of data measurement:</p> <p>The table below reports metrics concerning content LinkedIn removed from its platform as Misinformation, pursuant to the policy outlined in QRE 18.2.1 above. The metrics include:</p> <ul style="list-style-type: none"> – the number of pieces of content removed as Misinformation between 1 July – 31 December 2024, broken out by EEA Member State; – the number of those content removals that were appealed by the content author; – the number of those appeals that were granted; – the median time from appeal-to-appeal decision for those appeals. <p>The metrics are assigned to EEA Member State based on the IP address of the of the content author.</p>	<p>Methodology of data measurement:</p> <p>Bing Search does not have data relevant to this SLI. Users come to Bing Search with a specific research topic in mind and expect Bing Search to provide links to the most relevant and authoritative third-party websites on the Internet that are responsive to their search terms. Bing Search does not have a news feed for users of user content, allow users to post and share content within Bing, or otherwise enable content to go "viral" on Bing. See response to SLI 14.2.1 for relevant metrics.</p>

	The number of pieces of content removed as Misinformation between 1 July – 31 December 2024	The number of removals that were appealed by the content author	The number of appeals that were granted	The median time from appeal-to-appeal decision in hours	Total no of violations	Metric 1: indicating the impact of the action taken	Metric 2: indicating the impact of the action taken	Metric 3: indicating the impact of the action taken
Member States								
Austria	177	2	0	1.5 hours				
Belgium	445	3	1					
Bulgaria	36	0	0					
Croatia	54	3	0					
Cyprus	13	1	1					
Czech Republic	88	1	0					
Denmark	291	2	0					
Estonia	9	0	0					
Finland	52	1	0					
France	3,452	14	1					
Germany	1,639	40	2					
Greece	164	2	0					
Hungary	40	1	0					
Ireland	136	0	0					
Italy	1,264	15	2					
Latvia	7	0	0					
Lithuania	24	2	0					
Luxembourg	62	0	0					
Malta	11	1	0					
Netherlands	3,308	38	5					
Poland	128	2	0					
Portugal	189	5	1					
Romania	151	3	0					

Slovakia	8	0	0					
Slovenia	8	0	0					
Spain	640	6	1					
Sweden	209	1	0					
Iceland	6	0	0					
Liechtenstein	0	0	0					
Norway	99	2	0					
Total EU	12,605	142	14		N/A	N/A	N/A	N/A
Total EEA	12,710	144	14		N/A	N/A	N/A	N/A
Measure 18.3	LinkedIn				Bing Search			
QRE 18.3.1	<p>Microsoft maintains an internal research team — the Microsoft Threat Analysis Center (MTAC) — that conducts research on information influence operations and publishes both internal and public reports on its findings.</p> <p>Microsoft also works with Princeton University on the creation of hub for researchers to access data from social media companies to improve the identification and tracking of cyber enabled information operations. This accelerator will be available to researchers around the world including in Europe.</p>				<p>Bing Search regularly reviews and considers safe design practices and research and conducts user studies as part of its product and new feature development processes. Bing Search employees have actively partnered with Microsoft Research and third-party research organizations to contribute to novel research and internal studies concerning safe design practices, responsible AI, and disinformation.</p> <p>Bing also operates the Bing Qualified Researcher Program to enable EU researchers to request access for publicly accessible Bing data from a singular landing page.</p> <p>Microsoft also funds and works with Princeton University on the creation of hub for researchers to access data from social media companies to improve the identification and tracking of cyber enabled information operations. This accelerator will be available to researchers around the world including in Europe.</p> <p>Microsoft Research and Microsoft's AI for Good Lab regularly undertake and publish research that addresses or can be used in understanding online misinformation and disinformation. Microsoft researchers are currently</p>			

		<p>engaged in research leveraging search data to explore how medical hoaxes went viral during the COVID-19 pandemic and research concerning the detection of bias in mainstream news in connection with elections.</p> <p>Microsoft maintains an internal research team—the Microsoft Threat Analysis Center (MTAC)—that conducts research on information influence operations and publishes both internal and public reports on its findings. MTAC maintains global hubs and conducts intelligence analysis in over 13 languages. Additionally, Microsoft funds and works with external organizations to ingest data and research that they conduct into Microsoft products, including Bing Search.</p> <p>Bing Search looks forward to continued opportunities to contribute to and collaborate with the research community on future research and is in active discussions with third party organizations and the research community on best practices and mitigations for core web search and new generative AI experiences.</p>	
V. Empowering Users			
Commitment 19			
Relevant Signatories using recommender systems commit to make them transparent to the recipients regarding the main criteria and parameters used for prioritising or deprioritising information, and provide options to users about recommender systems, and make available information on those options.			
	C.19	M 19.1	M 19.2
We signed up to the following measures of this commitment:	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search
	LinkedIn	Bing Search	

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	No
If yes, list these implementation measures here [short bullet points].	New Implementation Measures Not applicable.	New Implementation Measures Not applicable.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures Not applicable	Planned Implementation Measures Bing regularly updates its policies and terms and conditions to account for product changes, user feedback, and evolving legal considerations.

Measure 19.1	LinkedIn	Bing Search
QRE 19.1.1	<p>LinkedIn has published a variety of articles to explain to users how our recommender systems work, including: "Mythbusting the Feed: How the Algorithm Works"; "Mythbusting the Feed: Helping our members better understand LinkedIn"; "Keeping your feed relevant and productive"; LinkedIn Safety Series: Using AI to Protect Member Data; "Guide: Features to Help You Control Your Feed and Conversations"; Our approach to building transparent and explainable AI systems; Suggested Posts in Feed. During earlier reporting periods LinkedIn collated and expanded upon existing resources to further explain the main parameters of LinkedIn recommender systems and options provided to users to influence and control these recommender systems.</p>	<p>Bing's search engine ranking algorithms are not a traditional "recommender system" in that Bing Search only provides content to users as a result of their express request, rather than pushing content to users who were not expressly seeking it. That said, the main parameters of Bing Search's ranking algorithms are published in the "How Bing Ranks Search Results" section of How Bing Delivers Search, which is available to Bing Search users in the EU. Bing Search also provides information on how it ranks and returns search suggestions in the Enhanced Search Experiences section of How Bing Delivers Search Results. Bing's ranking algorithms apply equally to traditional search results and generative AI features that extend to Bing.</p> <p>Please also see QREs 14.1.1, and 22.2.1.</p>

	<p>Additionally, LinkedIn addresses automated processing and relevancy in the LinkedIn User Agreement and it includes a link to the above referenced Help Centre article in Section 3.6 of the LinkedIn User Agreement, which section focuses on recommendations and automated processing. During an earlier reporting period, LinkedIn launched a new setting for members to control the default for how their LinkedIn feed is presented to them. Members can now change their preferred feed view from “most relevant first” to “most recent first”. “Most relevant first” means that LinkedIn will use data from the member’s profile and LinkedIn activity data to rank feed content based on the member’s interests. “Most recent first” means that LinkedIn will not use the member’s profile and LinkedIn activity data to rank feed content and will instead show updates from the member’s network in reverse chronological order.</p> <p>As reported in an earlier report, in August 2023, LinkedIn launched two new experiences in the EU. Additional detail is included below:</p> <ul style="list-style-type: none"> • LinkedIn launched a revised and expanded experience to enable Members to change how their Feed experience is presented to them. The choice is presented in the Feed (on desktop, mobile app, and mobile web) and it also points members to the setting referenced above where members can change the default sort of their Feed. Members can toggle between the following two choices: “most relevant first” or “most recent first.” The default sort option is “most relevant first.” If the Member toggles to “most recent first,” that choice will only persist for the current feed view on that particular device. • LinkedIn also launched a new setting within a Member’s Account Preferences settings so Members can change the default sort option from “most relevant first” to “most recent first.” Changing that setting will persist across sessions and devices. Members can learn more about this experience and the setting in our Help Center. 	
--	--	--

Measure 19.2	LinkedIn		Bing Search
SLI 19.2.1 – user settings	<p>Methodology of data measurement:</p> <p>Members that do not wish to have their LinkedIn feed experience sorted by relevance can change the default of how their LinkedIn feed experience is sorted via a setting.</p> <p>The table below reports: (1) the number of EEA members who used the “preferred feed view” setting between 1 July – 31 December 2024; and (2) the number of times those members used the “preferred feed view” setting between 1 July – 31 December 2024.</p> <p>The metrics are assigned to EEA Member State based on the self-reported profile location of the member.</p>		<p>Methodology of data measurement:</p> <p>Bing Search allows users to turn off search suggestions (including auto-suggest and related search suggestions) (“AS/RS”) in its user setting page, as shown below:</p> <div> <p>Search suggestions</p> <p><input checked="" type="checkbox"/> See search suggestions as you type</p> </div> <p>In the Bing image experience, users can turn off personalized search suggestions through the Settings pane. Bing anticipates providing reporting on utilization of this new measure in forthcoming reports.</p> <p>Users may also access, view, and delete their previous search queries in their Microsoft Account Privacy dashboard or clear their search history in Bing Search settings, which in turn will remove that content from any personalized search suggestions.</p> <p>Bing is currently building out expanded data retention and reporting functionalities related to this Commitment.</p>
	No of times users actively engaged with the “preferred feed view” setting		No of times users engaged with the search suggestion feature
Data	The number of EEA members who used the “preferred feed view” setting between 1 July – 31 December 2024	The number of times the members used the “preferred feed view” setting between 1 July – 31 December 2024	
Member States			
Austria	2,024	3,021	

Belgium	3,108	4,719	
Bulgaria	492	793	
Croatia	502	903	
Cyprus	256	391	
Czech Republic	1,179	1,742	
Denmark	2,495	3,760	
Estonia	294	444	
Finland	2,749	4,137	
France	21,112	33,303	
Germany	21,565	32,823	
Greece	1,305	2,031	
Hungary	777	1,148	
Ireland	2,757	4,212	
Italy	7,160	10,794	
Latvia	256	423	
Lithuania	387	606	
Luxembourg	460	686	
Malta	195	298	
Netherlands	13,698	21,132	
Poland	3,817	5,657	
Portugal	2,781	4,241	
Romania	1,357	2,269	
Slovakia	368	575	
Slovenia	268	389	
Spain	10,006	14,665	
Sweden	4,628	7,014	
Iceland	41	57	
Liechtenstein	24	44	
Norway	1,141	1,878	

Total EU	105,996	162,176	
Total EEA	107,202	164,155	81,409,838

V. Empowering Users

Commitment 20

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

	C.20	M 20.1	M 20.2
We signed up to the following measures of this commitment:	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search

	LinkedIn	Bing Search
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	Yes
If yes, list these implementation measures here [short bullet points].	<p>New Implementation Measures</p> <p>Not applicable</p>	<p>New Implementation Measures</p> <p>Microsoft has continued to improve content provenance measures on its AI image generation features, including continuing to pilot Content Integrity Tools that allowed users to add content credentials to their own authentic content (discussed further below).</p>
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No	Yes

If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures	Planned Implementation Measures
	Not applicable	Microsoft expects to continue its important work in content provenance tools and ways to help counter harmful AI-generated content.

Measure 20.1	LinkedIn	Bing Search
QRE 20.1.1	<p>Microsoft is a founding and active member of the Coalition for Content Provenance and Authenticity (C2PA) and is currently a co-chair.</p> <p>On 15 May 2024, LinkedIn announced that, starting that day, content containing the Coalition for Content Provenance and Authenticity's industry-leading "Content Credentials" technology (C2PA) will be automatically labelled on LinkedIn. Since LinkedIn began ramping Content Credentials, users are beginning to see the "Cr" icon on images and videos that contain C2PA metadata. By clicking on the icon, users are able to trace the origin of the AI-created media, including the source and history of the content, and whether it was created or edited by AI. The first place users will see the Content Credentials icon is on their LinkedIn feed, and LinkedIn is working to expand coverage to additional surfaces, including ads. By providing a verifiable trail of where content originates from and whether it was edited, C2PA helps keep digital information reliable, protect against unauthorized use, and create a transparent, secure digital environment for creators, publishers, and members. LinkedIn has also published an article in its Help Center which provides more information on C2PA and Content Credentials.</p>	<p>Microsoft and key members of the Bing Search team are also involved in the Partnership on AI ("PAI") to identify possible countermeasures against deepfakes and has participated in the drafting and refinement of PAI's proposed Synthetic Media Code of Conduct. The proposed Code of Conduct provides guidelines for the ethical and responsible development, creation, and sharing of synthetic media (such as AI-generated artwork).</p> <p>Microsoft is deeply focused on the potential risk that deepfakes and other abusive AI-generated content could be used to proliferate election-related misinformation, deceive the public, and potentially undermine trust in online content and our elections. For those reasons, we were a founding member of the Coalition for Content Provenance and Authenticity (C2PA). The C2PA is a coalition of technology companies, media, and others created to address the prevalence of misleading information online by developing technical standards to certify the source and history of media content. Pursuant to the C2PA specification, generative AI specifies techniques to add "Content Credentials" to online media consisting of metadata about the media's provenance and authenticity. In turn, that information provides consumers with a way to verify the history and trustworthiness of the media. Credentials are already added to all generative AI images created with our most popular consumer-facing AI image generation tools, including Image Creator, Microsoft Designer, and Copilot.</p>

		<p>In July 2023, Microsoft agreed to make a number of voluntary commitments related to furthering safe and trustworthy AI systems, including a commitment to deploy new state-of-the-art provenance tools to help the public identify AI generated audio-visual content and understand its provenance. See more at Our commitments to advance safe, secure, and trustworthy AI - Microsoft On the Issues.</p> <p>In addition, Microsoft has continued piloting Content Integrity Tools, which allowed users to add content credentials to their own authentic content. Designed as a pilot program primarily to support the 2024 election cycle and gather feedback about Content Credentials-enabled tools, during the reporting period of this report, the tools were available to political campaigns in the EU, as well as to elections authorities and select news media organizations in the EU and globally. These tools included a partnership and collaboration with fellow Tech Accord signatory, TruePic. Announced in April 2024, this collaboration leveraged TruePic's mobile camera SDK enabling campaign, election, and media participants to capture authentic images, videos and audio directly from a vetted and secure device. Called the "Content Integrity Capture App" (an app that makes it easy to directly capture images with C2PA enabled signing) launched for both Android and Apple and can be used by participants in the Content Integrity Tools pilot program.</p>
Measure 20.2	LinkedIn	Bing Search
QRE 20.2.1	<p>Microsoft is a founding member of the Coalition for Content Provenance and Authenticity (C2PA). The C2PA Coalition aims to address the prevalence of disinformation, misinformation, and online content fraud through developing technical standards for certifying the source and history or provenance of media content.</p>	<p>The Tech Accord's commitments make it more difficult for bad actors to use legitimate tools to create deepfakes and easier for users to identify authentic content. This focuses on the work of companies that generate AI content as well as those that distribute it and calls on them to strengthen the safety architecture in AI services by assessing risks and strengthening controls to help prevent abuse. For its part, Microsoft has taken steps to meet the</p>

	<p>As detailed in the response to QRE 20.1.1., LinkedIn has also adopted the C2PA’s industry-leading “Content Credentials” technology to include metadata labelling, including data about whether content is created using AI, on content containing the C2PA technology.</p> <p>Further information on C2PA is available on its website here.</p>	<p>commitments in the Tech Accord by further implementing content provenance, establishment of reporting channels, and improved detection capability. For example, Microsoft maintained launched a new web page – Microsoft-2024 Elections – where a political candidates and election authorities can report a concern about a deepfake of themselves deceptive AI targeting themselves or their election.</p> <p>Microsoft has worked to harness the data science and technical capabilities of our AI for Good Lab and MTAC teams to better assess whether abusive content—including that created and disseminated by foreign actors—is synthetic or not. Microsoft AI for Good lab has been developing detection models (image, video) to assess whether media was generated or manipulated by AI. The model is trained on approximately 200,000 examples of AI and real content. AI for Good continues to invest in creating sample dataset representing the latest generative AI technology. When appropriate, Microsoft calls on the expertise of Microsoft’s Digital Crimes Unit to invest in and operationalize the early detection of AI-powered criminal activity and respond appropriately, through the filing of affirmative civil actions to disrupt and deter that activity and through threat intelligence programs and data sharing with customers and government.</p>
--	--	---

V. Empowering Users				
Commitment 21				
Relevant Signatories commit to strengthen their efforts to better equip users to identify Disinformation. In particular, in order to enable users to navigate services in an informed way, Relevant Signatories commit to facilitate, across all Member States languages in which their services are provided, user access to tools for assessing the factual accuracy of sources through fact-checks from fact-checking organisations that have flagged potential Disinformation, as well as warning labels from other authoritative sources.				
	C.21	M 21.1	M 21.2	M 21.3

We signed up to the following measures of this commitment:	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn	LinkedIn Bing Search
--	---------------------------------	---------------------------------	-----------------	---------------------------------

	LinkedIn	Bing Search
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	No
If yes, list these implementation measures here [short bullet points].	New Implementation Measures Not applicable	New Implementation Measures Not applicable
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures Not applicable	Planned Implementation Measures Bing continues to evaluate additional tools and resources that support the spirit of this commitment.

Measure 21.1	LinkedIn	Bing Search
QRE 21.1.1	<p>As detailed above in QRE1.1.1 and 17.1.1, LinkedIn prohibits misinformation and disinformation on its platform, whether in the form of organic content or in the form of advertising content. LinkedIn's Professional Community Policies, which apply to all content on LinkedIn's platform, expressly prohibit the sharing of false or misleading content, including misinformation and disinformation.</p> <p>Where content is identified as misinformation (whether as a result of a report or proactively detected), we do not label it, rather it is removed from LinkedIn. This includes situations where LinkedIn</p>	<p>Bing Search provides a range of features and tools to help users determine the reliability of content displayed in Bing search results.</p> <p>Since 2017, Bing Search has ingested content from the public ClaimReview protocol made available through Schema.org and displayed fact check tags within search results for websites that have incorporated ClaimReview tags. ClaimReview functions as a tagging system that individual fact-checking organizations or media can use to identify their articles for search engines and social media platforms. Content tagged with a ClaimReview tag is "read" by Bing Search's search engine crawlers when ingesting websites for their</p>

	<p>personnel leverage the conclusions of fact checkers to determine whether the content at issue violates LinkedIn's Professional Community Policies.</p> <p>Please also see our response to QRE 17.1.1 which details how our internal team of experienced news editors provides trustworthy news about current events from verified sources and other steps we take to tackle disinformation.</p>	<p>index and is used by Bing Search to help promote and/or highlight fact-checked content in search results. See additional information at Bing adds Fact Check label in SERP to support the ClaimReview markup Webmaster Blog. Bing Search also utilizes ClaimReview and fact check data feeds from the from DataCommons.org.</p> <p>Fact-checks and articles from news and fact checking organizations may also appear as part of Bing Answers or similar features directed to users. In addition, news and fact-check articles can appear in Bing News verticals, which are often presented at the top of search results pages, depending on the user query.</p> <p>In addition to the resources discussed above, Bing maintains an additional fact-checking agreement to provide coverage in the following EEA languages: Bulgarian, Croatian, Czech, Dutch, English, Finnish, French, German, Greek, Hungarian, Polish, Portuguese, Romanian, Slovak, Spanish, and Swedish. In addition to the EU languages enumerated above, the fact-checking agreement also covers Catalan and Serbian languages, among others.</p> <p>Bing's generative AI features are subject to robust safety classifiers (which are informed by data shared by information integrity partners and other authority signals) to prevent the creation of low authority materials or disinformation. As Bing's generative AI features prohibit the creation of misleading content, and Bing does not allow users to publish or share content created by the system on the platform, in-product fact checks are not relevant to Bing's generative AI features. Moreover, generative responses are grounded in high authority web search results, and we provide links to websites so that users can learn more and evaluate the content for themselves.</p>
--	--	---

								For more information on other media literacy tools in Bing Search, please see QRE 17.1.1.
SLI 21.1.1 - actions taken under measure 21.1	<p>Methodology of data measurement:</p> <p>As detailed in our response to 21.1.1, LinkedIn removes, rather than labels, content that violates policy on false and misleading content.</p> <p>Accordingly, the metrics for this SLI for the period 1 July – 31 December 2024 is zero.</p>			<p>Methodology of data measurement:</p> <p>Bing Search uses the open schema.org ClaimReview protocol, and fact check articles incorporating ClaimReview tags are ingested in the Bing index. Bing cannot feasibly assess the location of the website or its operator for the purposes of this metric. Therefore, when calculating the location of fact checked content for the purposes of SLI, Bing has compiled the data as follows:</p> <p>“FCURL” represents the number of distinct URLs containing a ClaimReview tag (i.e. fact-check content) that appeared on the first page of Bing search results for any number of users located in the EU Member States and EEA.</p> <p>“FCI” represents number of times the above-mentioned URLs appeared on the first page of Bing search results to a user located in EU Member States and the EEA. Bing cannot provide data on the ratio of impressions of fact-checks to original impressions of fact-checked content, as Bing ingests websites with “fact check” tags and thus there is no ratio to assess. Bing also cannot reasonably quantify the “reach” of labels or fact checks available on its search index beyond what is provided below, as the appearance of fact checks depends entirely on each user’s unique search query.</p>				
	Total impressions of fact-checks	Ratio of impressions of fact-checks to original impressions of fact-checked content	Reach of labels/ fact-checkers and other authoritative sources	Other pertinent metric	Total impressions of fact-checks	Ratio of impressions of fact-checks to original impressions of fact-checked content	No of labels/ fact-checkers and other authoritative sources	Other pertinent metrics

				(N/A)	(FCI)	(N/A)	(FCURLs)	(N/A)
Member States								
Austria					34,509		4,698	
Belgium					60,454		5,999	
Bulgaria					2		2	
Croatia					1		1	
Cyprus					1		1	
Czech Republic					1		1	
Denmark					13,443		2,519	
Estonia					1		1	
Finland					9,591		1,629	
France					212,276		9,081	
Germany					3,968,924		17,342	
Greece					1		1	
Hungary					3		3	
Ireland					38,151		5,806	
Italy					68,653		5,939	
Latvia					1		1	
Lithuania					3		3	
Luxembourg					1		1	
Malta					0		0	
Netherlands					9,292		97,193	
Poland					59,184		4,690	
Portugal					38,493		4,212	
Romania					22		18	
Slovakia					1		1	
Slovenia					0		0	
Spain					161,600		7,793	
Sweden					39,686		5,756	

Iceland					6		6	
Liechtenstein					1		1	
Norway					23942		4,456	
Total EU					4,802,195		84,790	
Total EEA					4,826,144		89,253	

SLI 21.1.2 - actions taken under measure 21.1	Methodology of data measurement: As detailed in response to QRE 21.1.1, LinkedIn removes, rather than labels, content that violates our policy on false and misleading content. Accordingly, the metrics for this SLI for the period 1 July – 31 December 2024 is zero.			Methodology of data measurement: Metrics concerning “user interactions” and “labelling of content” are not applicable to Bing, as it is a search engine. Bing does not apply fact-check labels to websites; rather websites must embed a ClaimReview tag in order for Bing to ingest and display fact-check tags for a website within search results. Bing cannot quantify the number of articles published by independent fact-checkers that are available on the Bing Search index given the immense scale of search engine indexes. See SLI 21.1.1.		
	Nr of articles published by independent fact-checkers	Nr of labels applied to content, such as on the basis of such articles	Meaningful metrics such as the impact of 21.1. measures on user interactions with, or user re-shares of, content fact-checked as false or misleading	Nr of articles published by independent fact-checkers	Nr of labels applied to content, such as on the basis of such articles	Meaningful metrics such as the impact of 21.1. measures on user interactions with, or user re-shares of, content fact-checked as false or misleading

Measure 21.2	LinkedIn	This Measure is not relevant or pertinent to Bing Search as it does not host the content and cannot assess the extent to which content or indexed landing pages has reached its users.
--------------	-----------------	--

QRE 21.2.1	<p>LinkedIn has to date not undertaken and/or supported separate research and testing on the potential efficacy of warnings or updates targeted to users that have interacted with content that was later actioned upon for violation of our Professional Community Policies.</p> <p>Given LinkedIn currently removes, rather than labels, content that violates our policy on <u>false and misleading content</u>, LinkedIn may be unable to provide meaningful context to users as to the specific content that they had viewed which was later actioned.</p> <p>To the extent others have conducted such research and/or testing, LinkedIn is happy to discuss findings within the relevant Task-force Subgroups in view of identifying relevant follow-up actions.</p>	
Measure 21.3	LinkedIn	Bing Search
QRE 21.3.1	<p>As detailed in response to QRE 21.1.1, LinkedIn removes, rather than labels, content that violates our policy on <u>false and misleading content</u>.</p>	<p>Bing Search regularly consults research and evidence, including from internal Microsoft research and data science teams, related to safe design practices, labeling, and user experience and considers such research as part of its product design and testing. Bing Search also conducts internal research and user studies for product features, such as by analyzing impressions, engagement, or clicks of various features. Bing Search also has a “feedback” button easily accessible from any page of Bing. Bing Search reviews and may make improvements based on user feedback. Bing Search also regularly consults with third party organizations to hear feedback about product design and related safety considerations.</p> <p>As to fact check labels, Bing Search participated in the W3C organization that helped to design and promote Schema.org and ClaimReview and</p>

		<p>regularly meets with stakeholders to discuss common issues, including whether updates to these common schemas are necessary.</p> <p>Microsoft's Responsible AI team and product teams have worked to develop labeling and warning systems – as well as robust support and educational resources – to help ensure users are informed that AI-powered answers can have inaccuracies and to encourage users to consult the source links provided. Microsoft's Responsible AI team is staffed by a cross-disciplinary team of experts in AI, who consult regularly with external experts in the field to ensure our labels and warnings are designed in accordance with best practices.</p>
--	--	--

V. Empowering Users

Commitment 22

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

	C.22	M 22.1	M 22.2	M 22.3	M 22.4	M 22.5	M 22.6	M 22.7
We signed up to the following measures of this commitment:	LinkedIn Bing Search	LinkedIn	LinkedIn Bing Search	LinkedIn Bing Search				LinkedIn Bing Search

	LinkedIn	Bing Search
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	No

If yes, list these implementation measures here [short bullet points].	New Implementation Measures Not applicable	New Implementation Measures Not applicable.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No	No
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures Not applicable.	Planned Implementation Measures Bing regularly evaluates opportunities to improve its product and educate users on the trustworthiness and limitations of AI.

Measure 22.1	LinkedIn	This Measure is not relevant or pertinent to Bing Search as it does not allow users to share content.
QRE 22.1.1	<p>In October 2022, LinkedIn began offering an “About this profile” feature that shows members when a Profile was created, when the member’s contact information and Profile photo were last updated, and if the member has verifications associated with their profile (like a workplace or identity verification). LinkedIn also has rolled out a range of free verifications, which allow our members to verify certain information about themselves, like their association with a particular company or educational institution or their identity (through one of LinkedIn’s verification partners e.g. in the EEA LinkedIn’s identity verification partner is Persona).</p> <p>The above features can be strong user empowerment tools. Specifically, they can provide our members valuable authenticity signals to help them make more informed decisions about what content and individuals they engage with online.</p>	
	Methodology of data measurement:	

SLI 22.1.1 - actions enforcing policies above	<p>The table below reports metrics concerning EEA member use of the “About this profile” feature described above in QRE 22.1.1. The metrics include: (1) the number of members who used the “About this profile” feature between 1 July – 31 December 2024; and (2) the aggregate number of times those members used the feature between 1 July – 31 December 2024.</p> <p>The metrics are assigned to EEA Member State based on the self-reported profile location of the member.</p>		
	Percentage of users that have enabled the trustworthiness indicator	The aggregate number of times those members used the feature between 1 July – 31 December 2024	
	The number of members who used the “About this profile” feature between 1 July – 31 December 2024		
Member States			
Austria	201,047	497,213	
Belgium	416,378	1,008,087	
Bulgaria	67,997	173,071	
Croatia	49,369	107,802	
Cyprus	34,730	102,045	
Czech Republic	153,427	381,771	
Denmark	331,225	805,215	
Estonia	29,112	79,910	
Finland	146,719	330,688	
France	2,773,641	7,030,529	
Germany	1,754,780	4,557,455	
Greece	162,018	420,517	
Hungary	98,215	228,240	
Ireland	242,133	620,914	
Italy	1,186,530	2,655,054	

Latvia	31,247	74,767	
Lithuania	57,795	162,218	
Luxembourg	47,455	131,560	
Malta	24,417	62,099	
Netherlands	1,236,806	3,065,899	
Poland	508,088	1,319,937	
Portugal	326,189	770,593	
Romania	188,243	461,845	
Slovakia	46,635	114,738	
Slovenia	28,765	63,266	
Spain	1,253,059	3,172,615	
Sweden	437,507	1,037,882	
Iceland	7,395	15,305	
Liechtenstein	2,915	7,234	
Norway	168,496	369,054	
Total EU	11,833,527	29,435,930	
Total EEA	12,012,333	29,827,523	

Measure 22.2	LinkedIn	Bing Search
QRE 22.2.1	<p>LinkedIn does not prioritise any new sources in our feed, but in crisis situations, (e.g., Ukraine), we will use our manually curated Trusted Storylines to point members to reputable sources of information.</p> <p>LinkedIn's focus, in addition to pointing members to trustworthy content, has been to prohibit members from sharing harmful content on the platform. As a real identity online professional networking platform, content posted by members is seen by that member's colleagues, employer, and potential business partners. Consequently, members do not tend to post reputationally harmful content like misinformation, and such content does not gain traction on LinkedIn</p>	<p>Bing Search utilizes a variety of signals – including from trusted third parties as one of several means to help determine the authority score of a given website and rank it accordingly in search results.</p> <p>Bing Search also relies upon signals to help ensure that its search systems and features, such as auto-suggest and related search functions, direct users to high authority, trustworthy results and do not inadvertently suggest low authority or misleading content.</p>

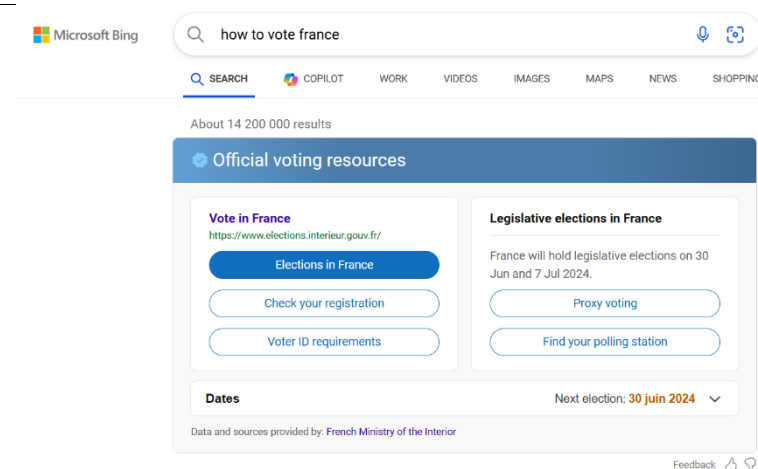
	for the same reasons. Nonetheless, where misinformation is removed from LinkedIn, it is ineligible to be included in our recommender systems.	The above mechanisms and the Bing algorithm's emphasis on promoting high authority content are applied equally to the new Bing generative AI features to help ensure that users are protected from inadvertently being exposed to harmful or low authority information in the new Bing experience.
Measure 22.3	LinkedIn	Bing Search
QRE 22.3.1	<p>In addition to the LinkedIn User Agreement, LinkedIn has established and published (a) the LinkedIn Professional Community Policies to set out and elaborate on LinkedIn's requirements and expectations for its member base; and (b) help center content that collates and expands upon existing resources to further explain the main parameters of LinkedIn recommender systems and options provided to users to influence and control these recommender systems.</p> <p>The Professional Community Policies and help center content are published on our platform and available in all languages that LinkedIn currently supports, including the following official EU and EEA languages: English, Czech, Danish, Dutch, Finnish, French, German, Greek, Hungarian, Italian, Norwegian, Polish, Portuguese, Romanian, Spanish and Swedish. Additionally, we have extended this language coverage in accordance with the Digital Services Act.</p> <p>LinkedIn seeks to reflect the best version of professional life through a community where we treat each other with respect and help one another succeed.</p> <p>The Professional Community Policies have three main elements: (1) Be Safe, (2) Be Trustworthy and (3) Be Professional. Additionally, the Professional Community Policies set out how members can report content that may violate our policies and that a violation of our Professional Community Policies can result in action taken against that member's account or content.</p>	<p>The above-mentioned policies and measures are available to EU users in EU languages through the Microsoft Bing Webmaster Guidelines and How Bing delivers search results.</p>

	<p>(1) Be Safe: do not post harassing content; do not threaten, incite, or promote violence; do not share material depicting the exploitation of children; do not promote, sell or attempt to purchase illegal or dangerous goods or services; do not share content promoting dangerous organisations or individuals.</p> <p>(2) Be Trustworthy: do not share false or misleading content; do not create a fake profile or falsify information about yourself; do not scam, defraud, deceive others.</p> <p>(3) Be Professional: do not be hateful, do not engage in sexual innuendos or unwanted advances; do not share harmful or shocking material; do not spam members or the platform.</p>	
Measure 22.4	This measure is aimed specifically at “providers of trustworthiness indicators” and is therefore not relevant or pertinent to Microsoft and its services.	This measure is aimed specifically at “providers of trustworthiness indicators” and is therefore not relevant or pertinent to Microsoft and its services.
QRE 22.4.1		
SLI 22.4.1 – actions enforcing policies above		
Measure 22.5	This measure is aimed specifically at “providers of trustworthiness indicators” and is therefore not relevant or pertinent to Microsoft and its services.	This measure is aimed specifically at “providers of trustworthiness indicators” and is therefore not relevant or pertinent to Microsoft and its services.
QRE 22.5.1		
SLI 22.5.1 – actions enforcing policies above		
SLI 22.5.2 – actions enforcing policies above		

Measure 22.6	This measure is aimed specifically at “providers of trustworthiness indicators” and is therefore not relevant or pertinent to Microsoft and its services.	This measure is aimed specifically at “providers of trustworthiness indicators” and is therefore not relevant or pertinent to Microsoft and its services
QRE 22.6.1		
SLI 22.6.1 – actions enforcing policies above		
Measure 22.7	LinkedIn	Bing Search
QRE 22.7.1	<p>As the world around us changes, LinkedIn continues to evolve and adapt our systems and practices for combating misinformation and other inauthentic behaviour on our platform, including to respond to the unique challenges presented by world events.</p> <p>LinkedIn’s Professional Community Policies, which all members agree to abide by on joining LinkedIn, prohibit misinformation. As described in more detail in our response to QRE 18.1.1, LinkedIn uses a combination of automated and manual activity to keep content that violates our policies off of LinkedIn.</p> <p>LinkedIn also aims to educate its members about civic discourse, electoral processes, and public security through its global team of news editors. These editors provide trustworthy and authoritative content to LinkedIn’s member-base, and its content moderation teams closely monitor associated platform conversations in a number of languages.</p> <p>In addition to broader measures, LinkedIn has taken special care to counter low authority information in relation to the Russian Invasion of Ukraine, the Israel-</p>	<p>In addition to broader measures described in this report, Bing Search has taken special care to address low authority information and misinformation in relation to elections, the Russian invasion of Ukraine, the Israel-Hamas conflict, and EU elections as detailed below and further in the Crisis Reporting appendices.</p> <p>Microsoft is also an active participant in the elections working group established by the Crisis Response Working Group. In addition, Microsoft works with election authorities responsible for running elections to promote trusted information regarding elections and monitors for foreign information operations targeting elections. Bing has launched special features such as info panels and specialized answers directing users to high authority content concerning elections and voting (see below example for France’s “snap” parliamentary election).</p>

Hamas Conflict and the European Elections as detailed in the Crisis Reporting appendices.

For example, during pre-election cycles, LinkedIn relies on trusted and reputable publisher sources for featured shares, focusing on the policy impact on businesses and professionals around the EU. LinkedIn also curate's links to topical landing pages from trusted publishers to provide members with easy and reliable entry points to more detailed coverage. LinkedIn does not compete with trusted publishers for speed or depth of coverage, but instead aims to connect their existing coverage to LinkedIn members and their needs. During important events in European elections, this team provides manually curated and localised storylines.



Additional detail is provided in the Crisis Reporting appendix.

In response to Russia's invasion of Ukraine in 2022, Bing Search has closely monitored low authority information trend and is working to promote authoritative content related to the conflict.

- Bing Search has taken steps to algorithmically boost authority signals and has downgraded less authoritative information (see SLI 22.7.1). These queries are translated automatically into other languages supported by Bing Search and integrated into Bing's generative AI experiences.
- Bing search works with Microsoft's Democracy Forward, Threat Assessment Center (MTAC) and Threat Intelligence Center (MSTIC) to ensure access to signals regarding Russian cyber and information operations targeting Ukraine to inform potential algorithmic interventions both for traditional and generative AI search tools.
- Bing Search regularly partners with independent research organizations and nonprofit organizations to maintain threat intelligence and inform potential algorithmic interventions both for traditional and generative AI search tools.

		<ul style="list-style-type: none">• Bing Search also takes action to remove autosuggest and related search terms that have been found likely to lead users to low authority content. These measures have helped ensure that Bing Search is promoting authoritative news sources, timelines, and other factual information at the top of algorithmic search results and in Bing generative AI experiences.• Bing Search has also complied with EU sanctions orders requiring the removal of certain Russian media sources, such as Russia Today and Sputnik.						
SLI 22.7.1 - actions enforcing policies above	Methodology of data measurement: LinkedIn has no applicable metrics to report during this reporting period.				Methodology of data measurement: Bing has revised the SLI action descriptions below for accuracy with respect to the metrics provided pursuant to this Section. Please see below key metrics. Although defensive search actions are taken at a global level (and therefore applied in every Member State), Bing has endeavored to provide the additional following data for this SLI: <ul style="list-style-type: none">• “Defensive Interventions (RU/UA)” refers to the total number of queries entered by users that were addressed with defensive search interventions related to the Ukraine/Russia crisis during the Reporting Period.• “Impressions (RU/UA)” reflects the number of user impressions for queries searched by users where defensive search interventions related to the Ukraine/Russia crisis were applied during the Reporting Period.			
	Impressions	Clicks	CTR	Shares	Defensive Interventions (RU/UA)	Impressions (RU/UA)	CTR (N/A)	Shares (N/A)
	Member States							
Austria					3,453	47,947		
Belgium					5,014	65,142		
Bulgaria					11	22		
Croatia					2	2		
Cyprus					0	0		
Czech Republic					23	28		
Denmark					1,660	12,233		

Estonia					5	5		
Finland					1,496	10,619		
France					11,724	286,787		
Germany					14,319	60,1938		
Greece					6	7		
Hungary					4	4		
Ireland					3,587	33,749		
Italy					6,832	122,340		
Latvia					11	14		
Lithuania					3	3		
Luxembourg					0	0		
Malta					2	2		
Netherlands					61,22	53,143		
Poland					6,028	91,154		
Portugal					3,410	26,600		
Romania					4	5		
Slovakia					5	5		
Slovenia					0	0		
Spain					11237	313,141		
Sweden					4696	35,766		
Iceland					0	0		
Liechtenstein					0	0		
Norway					2,988	31,233		
Total EU					79,654	1,700,656		
Total EEA					82,642	1,731,889		

V. Empowering users			
Commitment 23			
Relevant Signatories commit to provide users with the functionality to flag harmful false and/or misleading information that violates Signatories policies or terms of service.			
	C.23	M 23.1	M 23.2
We signed up to the following measures of this commitment:	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search

	LinkedIn	Bing Search
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	No
If yes, list these implementation measures here [short bullet points].	New Implementation Measures Not applicable	New Implementation Measures Not applicable.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No	No
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures Not applicable.	Planned Implementation Measures Bing monitors user feedback and regularly evolves its product reporting process and forms in response to user feedback, new legal obligations, or product developments.

Measure 23.1	LinkedIn	Bing Search
QRE 23.1.1	<p>If LinkedIn users locate content they believe violates our Professional Community Policies, we encourage them to report it using the in-product reporting mechanism represented by the three dots in the upper right-hand corner of the content itself on LinkedIn.</p> <p>Misinformation is specifically called out as one of the reporting options.</p> <p>The reporting feature is available through, and largely identical across, LinkedIn's website and mobile app, although reporting reasons and their visual presentation may vary slightly for certain types of content. In most instances, the reporting process is located just one click away from the content being reported and, depending on whether content is reported in the LinkedIn App or on desktop, the reporting process takes between four or five clicks to complete.</p> <p>Reported content generally is reviewed by trained content reviewers. In addition, LinkedIn uses automation to flag potentially violative content to our content moderation teams. If reported or flagged content violates the Professional Community Policies, it will be actioned in accordance with our policies.</p> <p>When members use the above reporting process, they will receive an email acknowledging receipt of the report. The email includes a link to the report status page, which we update when we make a decision, including providing the opportunity to appeal. Logged-out users receive updates on their report by email and are also provided with the opportunity to appeal.</p>	<p>As a search engine that does not host or display user generated content, Bing Search does not have a reporting function for user generated content.</p> <p>Bing Search's Report a Concern Form permits users to report third-party websites for a variety of reasons including disclosure of private information, spam and malicious pages, and illegal materials.</p> <p>Bing Search's "Feedback" tool, which is accessible on the lower right corner on a search results page, allows users to provide feedback on search results (including a screenshot of the results page) to Bing Search. Depending on the nature of the feedback, Bing Search may take appropriate action, such as to engage in algorithmic interventions to ensure high authority content appears above low authority content in search results, remove links that violate local law or Bing policies, add answers, warnings or other media literacy interventions on certain topics, or remove autosuggest terms.</p> <p>As discussed in QRE 14.1.2, these tools have also been updated to make it easy for users to report problematic content they encounter in Bing's generative AI experiences by including the same "Feedback" button with direct links to the respective service's "Report a Concern" tool on the footer of each page</p>

	<p>Members also receive an email notifying them in the event their content actioned in accordance with our policies. The email includes a link to a notice page for additional details and resources. If the member believes that their content complies with our Professional Community Policies, they can ask us to revisit our decision by submitting an appeal by clicking on the link in the notice page.</p> <p>Further, LinkedIn has a dedicated process for those entities who have been awarded Trusted Flagger status in accordance with Article 22 of the Digital Services Act.</p>	
Measure 23.2	LinkedIn	Bing Search
QRE 23.2.1	<p>As noted in our response to QRE 23.1.1, content that is flagged as misinformation (whether reported or automatically detected) is removed from LinkedIn. LinkedIn has a quality assurance team that is dedicated to ensure the quality of our content review processes and decisions. For example, the quality assurance team performs quality checks, on a routine basis, the content moderation decisions that have previously been made. This also allows us to improve our processes and further strengthen our platform as a trusted source of information.</p> <p>Furthermore, as a real identity professional network, LinkedIn acts vigilantly to maintain the integrity of all accounts and to ward off bot and false account activity. LinkedIn enforces the policies in its User Agreement prohibiting the use of “bots or other unauthorized automated methods to access the Services, add or download contacts, send or redirect messages, create, comment on, like, share, or re-share posts, or otherwise drive inauthentic engagement” through:</p>	<p>See QRE 23.1.1. Bing Search generally does not experience issues with mass flagging of content or abuse of its reporting features. This concern appears more applicable to other types of services (e.g., social media and online media websites) or content outside the scope of this regulation that is more prone to mass flagging, such as copyright infringement. Bing Search engages in human review of reports submitted through its reporting functionality and evaluates each report consistent with its policies and procedures.</p>

	<ul style="list-style-type: none"> • Maintaining a dedicated Anti-Abuse team to research emerging trends and key risks and develop tools to address them • Using AI to detect inauthentic activity and communities of fake accounts • Using automated systems detect and block automated activity • Imposing limits on certain categories of activity commonly engaged in by bad actors • Conducting manual investigation and restriction of accounts engaged in automated activity • Maintaining 24/7 escalation paths to address any emerging issues. 	
--	---	--

V. Empowering users

Commitment 24

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

	C.24	M 24.1
We signed up to the following measures of this commitment:	LinkedIn	LinkedIn

	LinkedIn	Commitment 24 is not relevant or pertinent to Bing Search as it does
--	-----------------	--

		not allow the posting of user content that would require user appeals
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	Choose an item.
If yes, list these implementation measures here [short bullet points].	New Implementation Measures Not applicable	
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No	Choose an item.
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures Not applicable	

Measure 24.1	LinkedIn	Measure 24.1 is not relevant or pertinent to Bing Search as it does not allow the posting of user content that would require user appeals
QRE 24.1.1	<p>When a post, comment, reply, or article, is reported and found to go against our Professional Community Policies, we take appropriate actions to remove it and/or restrict accounts depending on the severity of violation.</p> <p>The author whose content we've actioned or account we've restricted will generally be notified when we take action. Notices are typically sent by email and contain a link to a notice page containing certain additional information (e.g., about the content at issue, the policy violated, the action LinkedIn has taken, redress info and, in most instances, a link to allow the individual to appeal LinkedIn's decision). If the author believes LinkedIn has made a mistake in actioning their content or restricting their account, the member can ask LinkedIn to take a second look by clicking the link to submit an appeal. In order to submit the appeal, the member must confirm that they have read the relevant LinkedIn policy (a link is provided to the relevant</p>	

	<p>policy, for example, LinkedIn's policy on false and misleading information) and confirm that having reviewed the content at issue, they believe it complies with the policy. LinkedIn reviews those appeals and notifies the member of its appeal decision. If the appeal is successful, we put the content back up on LinkedIn.</p> <p>Appeals made by members are treated the same regardless of whether they use LinkedIn's premium services.</p>				
SLI 24.1.1 - enforcement actions Data	<p>Methodology of data measurement (where appropriate insights on data provided)</p> <p>The table below reports metrics concerning content LinkedIn removed from its platform as Misinformation, pursuant to the policy outlined in QRE 18.2.1. The metrics include:</p> <ul style="list-style-type: none"> - (1) the number of pieces of content removed as Misinformation between 1 July – 31 December 2024, broken out by EEA Member State; - (2) the number of those content removals that were appealed by the content author; - (3) the number of those appeals that were granted; - (4) the median time from appeal to appeal decision for those appeals. The metrics are assigned to EEA Member State based on the self-reported profile location of the content author. 				
	The number of pieces of content removed as Misinformation between 1 July	The number of those content removals that were appealed by the content author	The number of those appeals that were granted	The number of removals that were appealed by the content author	

	– 31 December 2024.				
Member States					
Austria	177	0	0	1.5 hours	
Belgium	445	3	1		
Bulgaria	36	0	0		
Croatia	54	3	0		
Cyprus	13	1	1		
Czech Republic	88	1	0		
Denmark	291	2	0		
Estonia	9	0	0		
Finland	52	1	0		
France	3,452	14	1		
Germany	1,639	40	2		
Greece	164	2	0		
Hungary	40	1	0		
Ireland	136	0	0		
Italy	1,264	15	2		
Latvia	7	0	0		
Lithuania	24	2	0		
Luxembourg	62	0	0		
Malta	11	1	0		
Netherlands	3,308	38	5		
Poland	128	2	0		
Portugal	189	5	1		
Romania	151	3	0		
Slovakia	8	0	0		
Slovenia	8	0	0		
Spain	640	6	1		
Sweden	209	1	0		

Iceland	6	0	0		
Liechtenstein	0	0	0		
Norway	99	2	0		
Total EU	12,605	142	14		
Total EEA	12,710	144	14		

V. Empowering users			
Commitment 25			
In order to help users of private messaging services to identify possible disinformation disseminated through such services, Relevant Signatories that provide messaging applications commit to continue to build and implement features or initiatives that empower users to think critically about information they receive and help them to determine whether it is accurate, without any weakening of encryption and with due regard to the protection of privacy.			
	C.25	M 25.1	M 25.2
We signed up to the following measures of this commitment:	Commitment 25 is not relevant to Bing Search and LinkedIn.	N/A	N/A

VI. Empowering the research community

Commitments 26 - 29

VI. Empowering the Research Community

Commitment 26

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

	C.26	M 26.1	M 26.2	M 26.3
We signed up to the following measures of this commitment:	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search

	LinkedIn	Bing Search
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes	Yes
If yes, list these implementation measures here [short bullet points].	<p>New Implementation Measures</p> <p>Beta program to allow bonafide researchers to access public data for research on impact of misinformation and other online harms impacting the Union.</p>	<p>New Implementation Measures</p> <p>Bing released a specialized dataset of European Parliament election related queries in different EU languages for use by the research community and to support transparency. Researchers can apply using the form found here.</p>
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	<p>Planned Implementation Measures</p> <p>Not applicable.</p>	Planned Implementation Measures

		Bing is actively exploring additional mechanisms to meet this commitment and welcomes feedback from the research community and Commission on the types of data that would be most useful to the research community. Bing is working to provide additional open datasets and resources that may be used by the research community.
--	--	---

Measure 26.1	LinkedIn	Bing Search
QRE 26.1.1	<p>LinkedIn supports the aims of the research community and regularly provides information and data to the research community in a variety of ways.</p> <p>To date, we have made non-personal, aggregated data publicly available (data on gender equity in the workplace, data on green skills and jobs, data on industry and job skills, and data on engagement with labor markets and employment trends). Our goal with this action to enable researchers to understand the rapidly changing world of work through access to and use of LinkedIn data. Because much of our data is publicly available, the extent to which such data has been used for disinformation related research purposes cannot easily be ascertained.</p> <p>Additionally, LinkedIn is expanding its API access for public data for disinformation related research purposes. Information about the LinkedIn APIs are available to the public and researcher access is provided here.</p>	<p>Bing Search and Microsoft are dedicated to supporting the research community and regularly provide information and data to the research community in a variety of ways.</p> <p>Bing Search already provides researchers and the public with access to MS MARCO, a collection of datasets focused on deep learning in search that are derived from Bing Search queries and related data. Research organizations can gain access to the MS MARCO datasets instantaneously via the MS MARCO homepage. The MS MARCO dataset has been cited in numerous research papers since its release and has been utilized for a range of research issues, including in connection with misinformation and disinformation. Because the dataset is provided open source, the extent to which it has been used for disinformation related research purposes cannot easily be ascertained.</p> <p>Bing Search also provides researchers with access to ORCAS: Open Resource for Click Analysis in Search msmarco (microsoft.github.io), a click-based dataset associated with the TREC Deep Learning Track, which provides 18 million connections to 10 million distinct queries and is available to researchers.</p>

	<p>Finally, Microsoft is also a leader in research in Responsible AI and provides a range of tools and resources dedicated to promoting responsible usage of artificial intelligence to allow practitioners and researchers to maximize the benefits of AI systems while mitigating harms. For example, as part of its Responsible AI Toolbox, Microsoft provides a Responsible AI Mitigations Library, which enables practitioners to more easily experiment with different techniques for addressing failure (which could include inaccurate outputs), and the Responsible AI Tracker, which uses visualizations to show the effectiveness of the different techniques for more informed decision-making. These tools are available to the public and research community for free.</p>	<p>In 2020, Bing Search also shared a search dataset for Coronavirus Intent comprised of queries from all over the world that had an intent related to the Coronavirus or Covid-19 (e.g., searches for “Coronavirus updates Seattle” or “Shelter in place”) for use by researchers and the public. This data, which is divisible by country, is particularly relevant to misinformation research on public health issues and the COVID-19 pandemic, as it provides insights into how users sought information related to the coronavirus during the pandemic. The dataset was also posted to Azure Open datasets for Machine Learning, Tensorflow.org, and Kaggle. See additional information on the dataset at Extracting Covid-19 insights from Bing Search data Bing Search Blog.</p> <p>In 2024, Microsoft publicly released a new information rich dataset, MS MARCO Web Search dataset, leveraging Bing search data. This dataset closely mimics real-world web document and query distribution and provides rich information for various kinds of downstream tasks and encourages research in various areas. It also contains rich information from the web pages, such as visual representation rendered by web browsers, raw HTML structure, clean text, semantic annotations, language and topic tags labeled by industry document understanding systems, etc. MS MARCO Web Search further contains 10 million unique queries from 93 languages with millions of relevant labeled query-document pairs collected from the search log of the Microsoft Bing search engine to serve as the query set.</p> <p>Additionally, researchers who are registered webmasters may utilize Bing Search’s Keyword Tools and Backlinks Webmaster Tools to provide insights into search usage and keywords. Bing is also working on ways to provide deeper research access to the tool across the research community and hopes to provide updates in its next report.</p> <p>Bing Search also offers use of Bing APIs to the public, which include Bing Image Search, Bing News Search, Bing Video Search, Bing Visual Search, Bing Web</p>
--	--	--

	<p>Search, Bing Entity Search, Bing Autosuggest, and Bing Spell Check. Bing Search provides free access to these APIs for up to 1,000 transactions per month, which may be leveraged by the research community.</p> <p>In addition to the above datasets, Microsoft Research maintains a public portal of codes, APIs, software development kits, and datasets that are available to the Research Community at Researcher tools: code & datasets - Microsoft Research. These public research tools can be accessed by researchers and downloaded instantaneously without formal applications or login credentials.</p> <p>Bing launched a Qualified Researcher Program to enable EU researchers to easily request access for publicly accessible Bing data from a singular landing page. However, because these datasets are already available open-source (see below), we expect some researchers may elect to obtain datasets via the above means to avoid the burden of an application and credentialing process.</p> <p>Bing compiled a specialized dataset of European Parliament election related queries in different EU languages for use by the research community and to support transparency; researchers can apply using the form found here. Additionally, Bing has engaged with European researchers to discuss the types of data that will be most useful to the research community.</p> <p>Microsoft is also a leader in research in Responsible AI and provides a range of tools and resources dedicated to promoting responsible usage of artificial intelligence to allow practitioners and researchers to maximize the benefits of AI systems while mitigating harms.</p> <p>Lastly, given the open nature of the Bing Search index and public nature of search results, researchers can utilize Bing Search or Bing's generative AI experiences to run specific queries and analyze results (unlike social media which may require private accounts or connections between users to access certain materials).</p>
--	---

QRE 26.1.2	LinkedIn published information on its [Beta] Researcher Access Program researcher access to public data.		Bing Search will publish information as it continues to build further data research infrastructure pertinent to these commitments.	
SLI 26.1.1 - uptake of the tools and processes described in Measure 26.1	Methodology of data measurement: LinkedIn will publish information as it continues to build its data research program pertinent to these commitments.		Methodology of data measurement: Because the above-mentioned tools discussed in QRE 26.1.2 predate the Code of Practice and were provided open source without tracking mechanisms, Microsoft is working on developing improved usage tracking for these publicly accessible researcher tools and datasets.	
	Nr of users of public access 0 applications were approved under our Beta Art 40 process in the period covered by this report. Note: Unknown number of researchers who use our broadly available service to conduct research.	Other quantitative information on public access	Nr of users of public access	Other quantitative information on public access
Data				
Measure 26.2	LinkedIn		Bing Search	
QRE 26.2.1	See QRE 26.1.1		Unlike social media platforms, Bing Search does not have private user accounts or other personal data provided by users as contemplated by Measure 26.2. However, Bing does enable researcher access to data on the platform through a number of mechanisms, as described in QRE 26.1.1 and the research partnerships described in QRE 18.3.1. Researchers can also submit real-time queries in Bing Search and Copilot.	
QRE 26.2.2	See QRE 26.1.1		See QRE 26.2.1 and 26.1.1.	

<p>QRE 26.2.3</p>	<p>Access to Data: For access to LinkedIn APIs, a researcher needs to submit an application, meet criteria for approval and provide additional information necessary for us to assess their project. APIs including non-public data may be made available for research purposes based on special requests and the ability of the researcher to protect personal data pursuant to GDPR and relevant intellectual property rights. Upon approval, the researcher's application will be provisioned with the relevant APIs. In addition, access is available to anyone who visits the relevant LinkedIn site.</p> <p>For access to other data, researchers may be provided with datasets and information as part of research inquiries and research partnerships with LinkedIn. Researchers may contact LinkedIn to discuss research opportunities.</p>	<p>Currently, there is not an application process to access the MS MARCO, ORCAS, MS MARCO Web Search, or Bing Coronavirus Query datasets in their original download locations, as Microsoft intended to allow open and easy access to the public and research community without arduous credentialing or account creation processes. Users may freely access the datasets instantaneously through the MS MARCO and ORCAS websites and MS-MARCO-Web-Search and Bing Coronavirus Query pages on Github. No application or credentialing is required, but unfortunately this open source model makes tracking usage more challenging and requires investment in additional tooling.</p> <p>For Bing Search's Keyword Research tool, Researchers may add their website (new or existing) to Bing Search Webmaster Tools and can freely use Keyword Research – Bing Webmaster Tools or Backlinks – Bing Webmaster Tools. Bing Search APIs are accessible at Bing APIs and may be accessed by signing up for an account or requesting access through the Qualified Researcher Program discussed below.</p> <p>For the Bing Qualified Researcher Program, eligible EU researchers may request access for publicly accessible Bing data and APIs, including the resources mentioned above, through an application form. If their request meets the criteria highlighted on the application page, data will be made available for the approved research purpose. More details are available at Bing Qualified Researcher Program - Microsoft Support.</p> <p>Other Microsoft datasets, including datasets derived by Bing Search, are accessible at Researcher tools: code & datasets - Microsoft Research. These also do not require credentials and datasets may be freely downloaded by researchers.</p> <p>For other research data, researchers may be provided datasets and information as part of research partnerships with Microsoft Research. Researchers may contact Microsoft Research to discuss research opportunities.</p>
--------------------------	--	---

							<p>And of course, the Bing Search service, including Bing's generative AI experiences, are also public and may be used for a variety of research purposes without login or credentials.</p> <p>Microsoft is continuing to explore possibilities to streamline data access consistent with this provision and in accordance with Microsoft Research's longstanding data sharing and collaboration with the research community. Bing also regularly explores additional research partnerships</p>
SLI 26.2.1 - meaningful metrics on the uptake, swiftness, and acceptance level of the tools and processes in Measure 26.2	<p>Methodology of data measurement:</p> <p>LinkedIn has provided metrics relating to the number of applications to its Beta Researcher Access Program in the period covered by this report. Consideration of a number of these applications remains ongoing.</p>						<p>Methodology of data measurement:</p> <p>Bing does not gate access for most of its datasets and therefore this metric is inapplicable, as any individual may freely access the tools. Bing is working on approaches for better tracking of usage of publicly released datasets and APIs.</p> <p>Bing tracks applications to its Qualified Researcher Program and will provide additional reporting in its next report.</p> <p>"MSMARCO" under "Other Metrics" provides the total global number of downloads of the MS Marco database</p>
	No of monthly users	No of applications received	No of applications rejected	No of applications accepted	Average response time	Other metrics	<p>Other metrics</p> <p>MSMARCO</p>
	Data	52	47	0			8181
Measure 26.3	LinkedIn						Bing Search
QRE 26.3.1	<p>LinkedIn provides a comprehensive Help Center for assistance with other matters. LinkedIn endeavors to restore access and address any issues expeditiously.</p>						<p>Users can report issues accessing MS MARCO and ORCAS datasets to ms-marco@microsoft.com. Microsoft endeavors to restore access and address any issues with dataset access expeditiously.</p>

		<p>For Bing Search's Keyword Research tool, users can report issues by creating a support request ticket at Webmaster Support - Bing Webmaster Tools.</p> <p>Users may report issues with Bing API access at https://aka.ms/bingapisupport.</p>
--	--	---

VI. Empowering the research community

Commitment 27

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

	C.27	M 27.1	M 27.2	M 27.3	M 27.4
We signed up to the following measures of this commitment:	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search

	LinkedIn	Bing Search
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes	Yes
If yes, list these implementation measures here [short bullet points].	<p>New Implementation Measures</p> <p>Microsoft was an active participant in the EDMO Working Group for the Creation of an Independent Intermediary Body to Support Research on Digital Platforms.</p>	<p>New Implementation Measures</p> <p>Microsoft was an active participant in the EDMO Working Group for the Creation of an Independent Intermediary Body to Support Research on Digital Platforms.</p>
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No	No

If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures	Planned Implementation Measures
	Not applicable.	Not applicable.

Measure 27.1	LinkedIn	Bing Search
QRE 27.1.1	Microsoft has been a member of the Working Group for the Creation of an Independent Intermediary Body to Support Research on Digital Platforms. The Working Group started its work on 10 May 2023 under the coordination of the European Digital Media Observatory (EDMO). Its main task has been to develop an organizational model for a new independent intermediary body that will facilitate data sharing between digital platforms and independent, external researchers.	Microsoft supports the development of an independent third-party body, in line with the Digital Services Act, and the upcoming associated Delegated Regulation on data access provided for in the Digital Services Act. Microsoft has also been a member of the Working Group for the Creation of an Independent Intermediary Body to Support Research on Digital Platforms. The Working Group started its work on 10 May 2023 under the coordination of the European Digital Media Observatory (EDMO). Its main task has been to develop an organizational model for a new independent intermediary body that will facilitate data sharing between digital platforms and independent, external researchers.
Measure 27.2	LinkedIn	Bing Search
QRE 27.2.1	As the development of the independent third-party body has not yet been finalized, there was no funding allocated to the implementation of Measure 27.2 during the period covered by this report.	As the development of the independent third-party body has not yet been finalized, there was no funding allocated to the implementation of Measure 27.2 during the period covered by this report.
Measure 27.3	LinkedIn	Bing Search
QRE 27.3.1	As the development of the independent third-party body has not yet been finalized, no data was shared with this body for the purposes of research as outlined under Measure 27.3 during the period covered by this report.	As the development of the independent third-party body has not yet been finalized, no data was shared with this body for the purposes of research as outlined under Measure 27.3 during the period covered by this report.
SLI 27.3.1 – research projects vetted by the independent third-party body	Methodology of data measurement: As the development of the independent third-party body has not yet been finalized, no research projects were vetted by this body, as set out under Measure 27.3, during the period covered by this report.	Methodology of data measurement: As the development of the independent third-party body has not yet been finalized, no research projects were vetted by this body, as set out under Measure 27.3, during the period covered by this report.

	Nr of research projects for which they provided access to data Not applicable.	Nr of research projects for which they provided access to data Not applicable.
Data		
Measure 27.4	LinkedIn	Bing Search
QRE 27.4.1	<p>Microsoft is a leader in research in Responsible AI and provides a range of tools and resources dedicated to promoting responsible usage of artificial intelligence to allow practitioners and researchers to maximize the benefits of AI systems while mitigating harms. For example, as part of its Responsible AI Toolbox, Microsoft provides a mitigations library, which enables practitioners to experiment with different techniques to address the failure of AI systems (which could include the production of inaccurate outputs). We also provide the Responsible AI tracker, which uses visualizations to show the effectiveness of the different techniques for more informed decision-making. These tools are available to the public and research community for free.</p> <p>These are just a few of the examples of partnerships Microsoft forged with third parties to combat the creation and dissemination of deceptive AI-generated content targeted at our elections. Microsoft teams regularly engage with external stakeholders on these issues to inform our internal policies, practices, and standards, to improve our products, and to understand emerging threats.</p>	<p>Microsoft is working with leading academics and researchers to help us better detect, understand, and mitigate the risks to elections posed by deceptive media generated by AI. For instance, Bing worked with Princeton University to address the question of how to build scalable measurement techniques to evaluate deceptive AI in images.</p> <p>More broadly, Microsoft is a leader in research in Responsible AI and provides a range of tools and resources dedicated to promoting responsible usage of artificial intelligence to allow practitioners and researchers to maximize the benefits of AI systems while mitigating harms. For example, as part of its Responsible AI Toolbox, Microsoft provides a mitigations library, which enables practitioners to experiment with different techniques to address the failure of AI systems (which could include the production of inaccurate outputs). We also provide the Responsible AI tracker, which uses visualizations to show the effectiveness of the different techniques for more informed decision-making. These tools are available to the public and research community for free.</p> <p>These are just a few of the examples of partnerships Microsoft forged with third parties to combat the creation and dissemination of deceptive AI-generated content targeted at our elections. Microsoft teams regularly engage with external stakeholders on these issues to inform our internal policies, practices, and standards, to improve our products, and to understand emerging threats.</p>

VI. Empowering the research community

Commitment 28

Relevant Signatories commit to support good faith research into Disinformation that involves their services.

	C.28	M 28.1	M 28.2	M 28.3	M 28.4
We signed up to the following measures of this commitment:	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search

	LinkedIn	Bing Search
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes	Yes
If yes, list these implementation measures here [short bullet points].	<p>New Implementation Measures</p> <p>Published details on our [Beta] Researcher Access Program</p>	<p>New Implementation Measures</p> <p>Microsoft and IE University's Center for the Governance of Change in Spain collaborate on AI4Democracy to create knowledge and promote action for a responsible use of artificial intelligence to defend and strengthen democracy. Launched in November 2023, AI4Democracy is ongoing and the continuation of the Tech4Democracy program, an initiative led by IE University in partnership with the United States Department of State and with the strategic support of Microsoft.</p>

Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	<p>Planned Implementation Measures</p> <p>Ongoing review of researcher feedback and needs may result in additional measures and resources being made available.</p> <p>Update our program in light of regulatory guidance that may be provided pursuant to Art. 40 of the DSA, including the upcoming delegated act on access to online platform data for vetted researchers.</p>	<p>Planned Implementation Measures</p> <p>Ongoing review of researcher feedback and requests may result in additional measures and resources.</p> <p>In addition, Microsoft Research regularly explores potential partnerships with third party research institutions and is actively in discussions with several research institutions on potential misinformation and disinformation related research that may leverage Bing Search data. Microsoft's internal research divisions also regularly initiate and support research relevant to misinformation and disinformation.</p>

Measure 28.1	LinkedIn	Bing Search
QRE 28.1.1	<p>LinkedIn facilitates research, engages with the research community, and provides data to the research community in a variety of ways, as described below and in QRE 26.1-2.</p> <p>Historically, LinkedIn's work with external stakeholders, including, for example, research institutes, and academia, to understand the rapidly changing world of work through access to and use of</p>	<p>Bing Search facilitates research, engages with the research community, and provides data to the research community in a variety of ways, as described below and in QRE 26.1-2 and 18.3.1.</p> <p>More broadly, Microsoft dedicates significant resources to supporting, promoting, and developing research on emerging issues including responsible AI, safe design, search and information retrieval, language</p>

	<p>LinkedIn data. Additionally, LinkedIn employs academics to gain practical experience combining industry knowledge with academic expertise to solve complex business problems spanning all areas of engineering, with an initial focus on artificial intelligence (including work related to large recommender systems and deep learning algorithms) and data science.</p> <p>While the foregoing work remains critical to our mission, we are working to expand access to data for research purposes consistent with the goals of the CoP as well as the applicable requirements of the DSA and look forward to providing further information on this in future reports.</p> <p>Additionally, LinkedIn regularly explores potential partnerships with non-governmental and research institutions and is actively in discussions with one research institution to conduct a data and recommender system pilot project leveraging LinkedIn data. LinkedIn hopes to publicly announce this partnership in its next report.</p> <p>Finally, LinkedIn has in place the needed teams and tools to make data available to researchers in a variety of ways, including via Excel or XML files, GitHub repositories, sandboxed laptops, and APIs.</p>	<p>learning models, and algorithms. Microsoft Research and other research groups within the company, such as the AI for Good Research Lab, employ robust teams of researchers and data scientists and regularly utilize Bing Search datasets and web search as part of important research efforts, including research focused on misinformation and/or disinformation.</p> <p>Microsoft Research and the AI for Good Lab regularly explore potential partnerships with third party research institutions and are actively in discussions with research institutions on potential misinformation and disinformation related research that may leverage Bing Search data. Microsoft also works with Princeton University to increase researcher access to data on cyber enabled influence operations.</p> <p>Microsoft Research also established the Accelerate Foundation Models Research (AFMR) global network and resource platform to assemble an interdisciplinary research community around solving some of today's greatest technical and societal challenges through aligning AI with shared human goals, values, and preferences; improving human-AI interactions; and accelerating scientific discoveries.</p> <p>Microsoft is currently undertaking additional research and education on how users interact with content provenance tools and the use of content provenance tools for AI including through its grant with C2PA..</p> <p>Microsoft Research has also undertaken research related to information integrity and elections in the age of generative AI.</p> <p>Lastly, Bing Search regularly partners with third party nonprofits and research organizations and NGO partners to review and evaluate emerging trends, techniques, tactics, and threat intelligence in misinformation and/or disinformation and related topics.</p>
--	---	---

Measure 28.2	LinkedIn	Bing Search
QRE 28.2.1	Please see QRE 26.1.1 and QRE 26.2.3.	See QRE 26.2.3 and 26.1.1.
Measure 28.3	LinkedIn	Bing Search
QRE 28.3.1	We look forward to partnering with other relevant signatories on this project and will provide further reporting as the annual consultation is established.	We look forward to partnering with other relevant signatories on this project and will provide further reporting as the annual consultation is established.
Measure 28.4	LinkedIn	Bing Search
QRE 28.4.1	There were no relevant developments during the period covered by this report.	There were no relevant developments during the period covered by this report.

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.

	C.29	M 29.1	M 29.2	M 29.3
We signed up to the following measures of this commitment:	Commitment 29 is aimed specifically at the research community and is therefore not relevant or pertinent to Microsoft and its services.			

VII. Empowering the fact-checking community

Commitments 30 - 33

VII. Empowering the fact-checking community

Commitment 30

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

	C.30	M 30.1	M 30.2	M 30.3	M 30.4
We signed up to the following measures of this commitment:	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search

	LinkedIn	Bing Search
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	Yes
If yes, list these implementation measures here [short bullet points].	New Implementation Measures Not applicable	New Implementation Measures Bing entered agreements with independent organizations to improve language coverage across EEA Member States and languages.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No	No
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures Not applicable	Planned Implementation Measures Not applicable

Measure 30.1	LinkedIn	Bing Search
QRE 30.1.1	<p>LinkedIn has entered into a fact-checking arrangement with an external, independent global news agency. This relationship helps our internal content reviewers determine if user generated content violates LinkedIn's policy on false and misleading content.</p>	<p>Bing Search supports the schema.org ClaimReview fact-check protocol as part of its search ingestion, as discussed further in QRE 21.1.1.</p> <p>In addition to organic fact checks and fact check content leveraging ClaimReview tags that may surface in search results, articles from news and fact checking organizations may appear as part of specialized Bing Answers. In addition, news and fact-check articles can appear in Bing News carousels, which are often presented at the top of search results pages, depending on the nature of the user query. Microsoft maintains agreements with news publishers to surface high authority content, including articles from well-regarded fact checking organizations and journalist-driven fact-checks, high in relevant search results.</p>
QRE 30.1.2	<p>Reuters, a global news organization with 2,500 journalists in about 200 locations worldwide. Reuters is one of the largest news agencies in the world.</p>	<p>See QRE 30.1.1 and QRE 21.1.1. The trusted third-party partners Bing search leverages provide coverage in several EU languages, such as Bulgarian, Croatian, Czech, Dutch, English, Finnish, French, German, Greek, Hungarian, Polish, Portuguese, Romanian, Slovak, Spanish, and Swedish. In addition to the EU languages enumerated above, contracted fact-checking data also includes coverage of Catalan and Serbian languages.</p>
QRE 30.1.3	<p>LinkedIn has implemented internal processes empowering our hundreds of global internal content reviewers to be able to obtain a fact-check from an external fact-checker partnership. Fact-checker conclusions are reviewed by internal content reviewers to determine whether the content at issue violates LinkedIn's policy on false and misleading content and if so, the content is removed from the platform.</p>	<p>See QREs 30.1.1-2.</p> <p>As noted above, any authorized fact-checking organization can leverage the ClaimReview protocol to provide fact-checks to Bing Search. Bing Search would welcome additional usage of the ClaimReview protocols in EU Member States and actively partners with third party partners including, news organizations, fact checking organizations and nonprofits in the EU to inform defensive search interventions, threat intelligence, and issue monitoring. Bing has dedicated internal teams that leverage this information to inform product mitigations and defensive search interventions.</p>

SLI 30.1.1 - Member States and languages covered by agreements with the fact-checking organisations	<p>Methodology of data measurement:</p> <p>LinkedIn receives fact checking services for content in English, Spanish, Portuguese, French, German, Italian, Croatian, Czech, Danish, Dutch, Finnish, Greek, Hungarian, Polish, Swedish, Bulgarian, Latvian, Lithuanian, Maltese, Romanian and Slovak.</p> <p>LinkedIn sends content to external fact checkers regardless of the location of the member posting the content, the viewers of the content, or the topic at issue. Content that violates LinkedIn's policy on false and misleading content is removed.</p>	<p>Methodology of data measurement:</p> <p>As described in QRE 30.1.1, Microsoft has a number of news agreements that include journalism, news, and fact checking coverage and provide remuneration to fact checkers and news organizations for news that is surfaced on Bing. These agreements, the nature of which are confidential, cover a range of languages and markets, including EEA member states. While certain agreements include fact checking coverage, because these arrangements are not strictly for fact-checking services, we do not reflect these agreements in this SLI.</p> <p>In addition, as set out in QRE 30.1.2 and SLI 31.1.1, any fact-checking organisation can leverage the ClaimReview protocol to embed fact-check tags into their website (thereby adding fact-check tags or flags into indexed results) and there is no limitation in terms of languages and Member States covered. Because ClaimReview is an open protocol available for all websites and search engines to use, Bing does not have agreements with individual fact-checking organisations to tag articles in Claim Review.</p>
	Nr of agreements with fact-checking organisations	Nr of agreements with fact-checking organisations
EU	1	-

Measure 30.2	LinkedIn	Bing Search
QRE 30.2.1	<p>LinkedIn has engaged in arms-length negotiations with a large global news organisation that follows the highest ethical standards in news reporting, including those related to accuracy, independence, integrity, and freedom from bias. Our agreements give the fact-checkers complete discretion in providing their factchecking conclusions, and LinkedIn personnel leverage these conclusions to determine whether the content at issue violates</p>	<p>Microsoft provides fair compensation and has engaged in arms-length negotiations with news and fact-checking organizations to secure fact checking coverage in the EU, through news partnership arrangements that support Bing news product features, such as specialized answers and news carousels. These partners operate independently and Microsoft agreements respect their editorial independence.</p>

	LinkedIn's policy on false and misleading content and if so, the content is removed from the platform.	
QRE 30.2.2	LinkedIn meets with its fact-checking partner to discuss improvements in process.	<p>As noted above, Bing Search ingests ClaimReview tags embedded in fact-check content posted on websites that are indexed in the Bing Search index.</p> <p>Webmasters for fact-checking organizations have self-help tools available as part of Bing Search's Webmaster Tools, that allow them to review website analytics and search effectiveness (including insights into keywords or search queries used in Bing Search to reach their website) for websites containing ClaimReview tags . This dashboard provides website operators with a range of data and analytics that can be used by fact-checking organizations to assess how users found their fact-checked content, website traffic patterns, and the effectiveness of their fact-check tags.</p> <p>See QREs 30.1.1-2 for additional information on Bing Search's ClaimReview fact check program.</p> <p>Bing has also engaged in conversations with members of the fact-checking community and signatories to solicit feedback on search considerations and fact-checking.</p>
QRE 30.2.3	This QRE is not relevant or pertinent as LinkedIn is not a fact-checking organisation.	This QRE is not applicable to Bing Search, as it is not a fact-checking organization.
Measure 30.3	LinkedIn	Bing Search
QRE 30.3.1	LinkedIn meets with its fact-checking partner to discuss improvements in process.	Bing meets with its fact-checking partner to discuss improvements in process.
Measure 30.4	LinkedIn	Bing Search
QRE 30.4.1	There were no relevant developments during the period covered by this report.	There were no relevant developments during the period covered by this report.

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.

	C.31	M 31.1	M 31.2	M 31.3	M 31.4
We signed up to the following measures of this commitment:	LinkedIn Bing Search	LinkedIn	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn Bing Search

	LinkedIn	Bing Search
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Choose an item.No	No
If yes, list these implementation measures here [short bullet points].	New Implementation Measures No applicable	New Implementation Measures Not applicable
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No	No
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures Not applicable.	Planned Implementation Measures Not applicable

Measure 31.1	LinkedIn	This Measure is not relevant or pertinent to Bing Search as it does not showcase User Generated Content.
Measure 31.2	LinkedIn	Bing Search
QRE 31.1.1	<p>LinkedIn leverages its fact-checker to review user generated content that may violate its Professional Community Policies, which prohibit misinformation. Content that violates LinkedIn's Professional Community Policies is removed from LinkedIn.</p>	<p>Articles from news and fact checking organizations may appear as part of specialized Bing Answers. In addition, news and fact-check articles can appear in Bing News carousels, which are often presented at the top of search results pages, depending on the nature of user query. Microsoft maintains agreements with news publishers to surface high authority content, including articles from well-regarded fact checking organizations and journalist-driven fact-checks, high in relevant search results.</p> <p>During the Reporting Period, Bing maintained a fact-checking agreement to provide coverage in the following EU languages: Bulgarian, Croatian, Czech, Dutch, English, Finnish, French, German, Greek, Hungarian, Polish, Portuguese, Romanian, Slovak, Spanish, and Swedish; the fact-checking agreement also includes coverage of Catalan and Serbian languages, among others.</p> <p>In addition, Bing uses threat intelligence to inform the Bing algorithm and defensive search measures used for Bing search and Bing's generative search features. Bing works with trusted third-party partners for leads of potential threats, including in EEA member state languages) to inform defensive search strategies for Bing. Bing also utilises the ClaimReview open protocol to ingest fact checks into search results.</p> <p>Bing has increased coverage of EEA languages, informing interventions across monitored themes and sources.</p> <p>In addition, Bing Search uses ClaimReview tags embedded in websites with fact-checked content to help inform its algorithms (i.e., by leading users to more authoritative sources of information) and to provide useful context and indications of trustworthiness to its users in search results.</p> <p>See QREs 21.1.1 and 30.2.1-2.</p>

SLI 31.1.1 - use of fact-checks	Methodology of data measurement:				Methodology of data measurement:			
	<p>The figure for the number of content pieces reviewed by fact-checkers represents the number of pieces sent to our external fact checkers during the period 1 July – 31 December 2024. See also SLI 21.1.2.</p>				<p>Fact Check URLs (“FC URL”) – This represents the number of distinct URLs containing a ClaimReview tag (i.e. fact-check content) that appeared on the first page of Bing search results for any number of users located in the EU Member States.</p> <p>Fact Check Impressions (“FCI”) – The number of times the above-mentioned URLs appeared on the first page of Bing search results to a user located in the EU Member States.</p>			
	Nr of fact-checked articles published	Reach of fact-checked	Nr of content pieces reviewed by fact-checkers	Other	Nr of fact-checked articles published	Reach of fact-checked (FCI)	Nr of content pieces reviewed by fact-checkers	Other (FC URL)
Member States								
Austria						34,509		4,698
Belgium						60,454		5,999
Bulgaria						2		2
Croatia						1		1
Cyprus						1		1
Czech Republic						1		1
Denmark						13,443		2,519
Estonia						1		1
Finland						9,591		1,629
France						212,276		9,081
Germany						3,968,924		17,342
Greece						1		1
Hungary						3		3
Ireland						38,151		5,806

Italy						68,653		5,939
Latvia						1		1
Lithuania						3		3
Luxembourg						1		1
Malta						0		0
Netherlands						97,193		9,292
Poland						591,84		4,690
Portugal						38,493		4,212
Romania						22		18
Slovakia						1		1
Slovenia						0		0
Spain						161,600		7,793
Sweden						39,686		5,756
Iceland						6		6
Liechtenstein						1		1
Norway						23,942		4,456
Total EU					N/A	4,802,195	N/A	84,790
Total EEA					N/A	4,826,144	N/A	89,253
Total Global	0	N/A	106					

SLI 31.1.2 - impact of actions taken	Methodology of data measurement:			Methodology of data measurement:		
	Not applicable as LinkedIn removes, rather than labels, content that violates our policy on false and misleading content .			Bing Search is not able to provide metrics concerning the “impact” of individual fact check websites appearing in its search results in response to specific queries.		
	Nr of pieces of content labelled	Impact of said measures on user interactions with information labelled	Other	Nr of pieces of content labelled	Impact of said measures on user interactions with information labelled as false or misleading	Other

		as false or misleading				
Total EEA	0	Not applicable		Not applicable	Not applicable	

SLI 31.1.3 – Quantitative information used for contextualisation for the SLIs 31.1.1 / 31.1.2	Methodology of data measurement:	Methodology of data measurement:
	Not applicable.	Not applicable.
	Denominator to be decided within the TF ahead of the baseline report	Denominator to be decided within the TF ahead of the baseline report
	Not applicable	Not applicable
Total EEA	Not applicable	Not applicable

Measure 31.3	LinkedIn	Bing Search
QRE 31.3.1	There were no discussions in the relevant Subgroup of the Permanent Task-force on the development of the repository of fact-checking content during the period covered by this report.	There were no discussions in the relevant Subgroup of the Permanent Task-force on the development of the repository of fact-checking content during the period covered by this report.
Measure 31.4	LinkedIn	Bing Search
QRE 31.4.1	There were no discussions in the relevant Subgroup of the Permanent Task-force on the development of the repository of fact-checking content during the period covered by this report.	There were no discussions in the relevant Subgroup of the Permanent Task-force on the development of the repository of fact-checking content during the period covered by this report.

VII. Empowering the fact-checking community

Commitment 32

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

	C.32	M 32.1	M 32.2	M 32.3
We signed up to the following measures of this commitment:	LinkedIn Bing Search	LinkedIn Bing Search	LinkedIn	LinkedIn Bing Search

	LinkedIn	Bing Search
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	No
If yes, list these implementation measures here [short bullet points].	New Implementation Measures Not applicable	New Implementation Measures Not applicable
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No	No
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures Not applicable	Planned Implementation Measures Not applicable

Measure 32.1	LinkedIn		Bing Search	
Measure 32.2	LinkedIn		This Measure is not relevant to Bing Search as it does not showcase User Generated Content.	
QRE 32.1.1	LinkedIn's Professional Community Policies prohibit misinformation, and LinkedIn will remove policy-violating content, after consulting with its fact-checking partners (if needed). LinkedIn provides its fact-checking partners with live links to content, which allows partners to easily determine whether that content was thereafter removed by LinkedIn.		See QREs 21.1.1 and 30.2.1-2.	
SLI 32.1.1 - use of the interfaces and other tools	Methodology of data measurement:		Methodology of data measurement:	
	Monthly users	Other	Monthly users	Other
Total EEA	Not applicable.			
Measure 32.3	LinkedIn		Bing Search	
QRE 32.3.1	LinkedIn currently uses the Code's Task-force, in particular the Crisis Response and Empowerment of Fact-checkers subgroups, as a channel of communication with the fact-checking community represented by the signatories to the Code.		Bing Search currently uses the Code's Task-force, in particular the Crisis Response and Empowerment of Fact-checkers subgroups, as a channel of communication with the fact-checking community represented by the signatories to the Code. We continue to explore ways in which we can further support information exchange with the fact-checking community.	

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.

C.33

M 33.1

We signed up to the following measures of this commitment:	Commitment 33 is aimed specifically at fact-checking organisations and therefore not relevant or pertinent to Microsoft and its services.	N/A
--	---	-----

VIII. Transparency Centre

Commitments 34 - 36

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	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No
If yes, list these implementation measures here [short bullet points].	Not applicable
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	<p>Planned Implementation Measures</p> <p>Microsoft is committed to the proper functioning of the Transparency Center website and will therefore continue its engagement in the Transparency Center subgroup in order to assess the necessity of technical adjustments and new actions to improve the website. Microsoft will thereby contribute to, where necessary, making the website more user-friendly and easily accessible for users ahead of the next reporting period.</p>
Measure 34.1	Microsoft Corporation
Measure 34.2	Microsoft Corporation
Measure 34.3	Microsoft Corporation
Measure 34.4	Microsoft Corporation
Measure 34.5	Microsoft Corporation

VIII. Transparency Centre	
Commitment 35	
Signatories commit to ensure that the Transparency Centre contains all the relevant information related to the implementation of the Code's Commitments and Measures and that this information is presented in an easy-to-understand manner, per service, and is easily searchable.	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	<p>New implementation Measures</p> <p>Microsoft will upload its March 2025 Report to the Transparency Centre website in a timely manner, which includes clear and simple information on the new or existing policies and actions that each service has implemented based on our Subscription document that is applicable to this reporting period.</p>
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	<p>Planned Implementation Measures</p> <p>Within the context of the work of the Transparency Center subgroup, Microsoft will assess the necessity of technical adjustments and contribute to actions where necessary, that are aimed at making the website more user-friendly and easily accessible for users ahead of the next reporting period.</p>

Measure 35.1	Microsoft Corporation
Measure 35.2	Microsoft Corporation
Measure 35.3	Microsoft Corporation
Measure 35.4	Microsoft Corporation
Measure 35.5	Microsoft Corporation
Measure 35.6	Microsoft Corporation

VIII. Transparency Centre	
Commitment 36	
Signatories commit to updating the relevant information contained in the Transparency Centre in a timely and complete manner.	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	<p>New implementation Measures</p> <p>By uploading this report, Microsoft updated the Transparency Centre with relevant information related to its new policies and implementation actions.</p>
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	<p>Planned Implementation Measures</p> <p>Microsoft is committed to providing regular updates as set out under Measures 36.1, 36.2 and 36.3.</p>

Measure 36.1	Microsoft Corporation
Measure 36.2	Microsoft Corporation
Measure 36.3	Microsoft Corporation
QRE 36.1.1 (for the Commitments 34-36)	The Transparency Centre was successfully launched in February 2023. We continue to upload our report according to the approved deadlines
QRE 36.1.2 (for the Commitments 34-36)	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) meaningful quantitative information on the usage of the Transparency Centre, such as the average monthly visits of the webpage.	Methodology of data measurement: Website metrics
Data	Between 1 July 2024 to 31 December 2024, the common Transparency Centre has been visited by 20,255 unique visitors. The Signatories' reports were downloaded 5,626 times by 1,275 unique visitors. More specifically, Microsoft's previous COPD report was downloaded 153 times by 82 unique users.

IX. Permanent Task-Force

Commitment 37

IX. Permanent Task-Force	
Commitment 37	
<p>Signatories commit to participate in the permanent Task-force. The Task-force includes the Signatories of the Code and representatives from EDMO and ERGA. It is chaired by the European Commission, and includes representatives of the European External Action Service (EEAS). The Task-force can also invite relevant experts as observers to support its work. Decisions of the Task-force are made by consensus.</p>	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	<p>New implementation Measures</p> <p>Microsoft has actively engaged in and contributed to the work of the Task-force and relevant Subgroups and Working Groups that were active during the reporting period.</p>
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	<p>Planned Implementation Measures</p> <p>Microsoft is committed to continuing its active engagement in and contribution to the Task-force and service relevant Subgroups and Working Groups in the upcoming six-month period.</p>

Measure 37.1	Microsoft Corporation
Measure 37.2	Microsoft Corporation
Measure 37.3	Microsoft Corporation
Measure 37.4	Microsoft Corporation
Measure 37.5	Microsoft Corporation
Measure 37.6	Microsoft Corporation
QRE 37.6.1	<p>Microsoft has actively engaged in and contributed to all the Task-force Plenary meetings as well as to the meetings of all Subgroups and Working Groups active in the current reporting cycle under the Task-force.</p> <p>As part of each Subgroup and Working Group that has taken place during the reporting period, Microsoft has actively contributed to the development of the deliverables that were collectively agreed.</p> <p>Microsoft has continuously engaged with all Signatories of the Code, offering its perspectives on issues unique to its subscribed services and responding to ad-hoc inquiries related to various actions taken by its subscribed services. Microsoft appreciates the added value and insights that the Task-Force has created for each Signatory individually as well as the collective community of Signatories. Microsoft looks forward to continue its constructive cooperation within the Code of Practice's governance framework as relevant.</p>

X. Monitoring of Code

Commitment 38 - 44

X. Monitoring of Code	
Commitment 38	
The Signatories commit to dedicate adequate financial and human resources and put in place appropriate internal processes to ensure the implementation of their commitments under the Code.	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	<p>New implementation Measures</p> <p>A dedicated cross-company team continues to ensure proper tracking and compliance with the Code of Practice across all applicable geographical areas, consisting of relevant product members from all subscribed services, attorneys, members of the European Government Affairs team and Democracy Forward Team. Budget items from across Microsoft teams have been used to ensure compliance including ongoing investment in trusted third parties.</p>
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No
If yes, which further implementation measures do you plan to put in place in the next 6 months?	<p>Planned Implementation Measures</p> <p>Not applicable</p>
Measure 38.1	Microsoft Corporation
QRE 38.1.1	Microsoft has a dedicated cross-company team to ensure proper tracking and compliance with the Code of Practice across all applicable geographical areas, consisting of relevant product members from all subscribed services as well as relevant lawyers, members of the European Government Affairs team and Democracy Forward Team. In addition, we implemented an internal tracking process that captured all relevant commitments, responsible entity and persons responsible for compliance with the Code of Practice. Moreover, regular review of new product features take place to assess potential impacts and compliance under the Code.

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.	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No
If yes, list these implementation measures here [short bullet points].	<p>New implementation Measures</p> <p>This Commitment is only relevant for the Baseline Reports, which were provided to the European Commission in January 2023.</p>
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No
If yes, which further implementation measures do you plan to put in place in the next 6 months?	<p>Planned Implementation Measures</p> <p>Not applicable.</p>

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.	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No

If yes, list these implementation measures here [short bullet points].	New implementation Measures Not applicable
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures Not applicable
Measure 40.1	Microsoft Corporation
Measure 40.2	Microsoft Corporation
Measure 40.3	Microsoft Corporation
Measure 40.4	Microsoft Corporation
Measure 40.5	Microsoft Corporation
Measure 40.6	Microsoft Corporation

X. Monitoring of Code	
Commitment 41	
<p>Signatories commit to work within the Task-force towards developing Structural Indicators, and publish a first set of them within 9 months from the signature of this Code; and to publish an initial measurement alongside their first full report. To achieve this goal, Signatories commit to support their implementation, including the testing and adapting of the initial set of Structural Indicators agreed in this Code. This, in order to assess the effectiveness of the Code in reducing the spread of online disinformation for each of the relevant Signatories, and for the entire online ecosystem in the EU and at Member State level. Signatories will collaborate with relevant actors in that regard, including ERGA and EDMO.</p>	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	<p>New implementation Measures</p> <p>The second report on Structural Indicators by TrustLab was published in September 2024.</p>
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No
If yes, which further implementation measures do you plan to put in place in the next 6 months?	<p>Planned Implementation Measures</p> <p>Not applicable.</p>
Measure 41.1	Microsoft Corporation
Measure 41.2	Microsoft Corporation
Measure 41.3	Microsoft Corporation

X. Monitoring of Code	
Commitment 42	
Relevant Signatories commit to provide, in special situations like elections or crisis, upon request of the European Commission, proportionate and appropriate information and data, including ad-hoc specific reports and specific chapters within the regular monitoring, in accordance with the rapid response system established by the Taskforce.	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	<p>New implementation Measures</p> <p>During the reporting period, Microsoft has been an active participant in and contributor to the Task-force's Elections Working Group, in particular in view of elections that took place in the EU as well as in the context of ongoing discussions towards an Elections Rapid Response System.</p>
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	<p>Planned Implementation Measures</p> <p>Microsoft will continue its participation in the Task-force's Crisis Response Subgroup and Elections Working Group, as relevant.</p>

X. Monitoring of Code	
Commitment 43	
Signatories commit to produce reports and provide data following the harmonised reporting templates and refined methodology for reporting and data disclosure, as agreed in the Task-force.	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	<p>New implementation Measures</p> <p>Microsoft has provided its March 2025 Report in accordance with the revised Harmonised Reporting Template and underlying methodologies as jointly developed by Signatories in the Monitoring and Reporting Subgroup under the Code's Task-force.</p>
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	<p>Planned Implementation Measures</p> <p>Microsoft will continue its active engagement in the respective Task-force Subgroups to keep the Harmonised Reporting Template and underlying methodologies up to date, where necessary in view of its experience with reporting.</p>

X. Monitoring of Code**Commitment 44**

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

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No
If yes, list these implementation measures here [short bullet points].	New implementation Measures Not applicable.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Planned Implementation Measures Not applicable

Reporting on the services' response during a period of crisis

Reporting on the services' response during a crisis

War of aggression by Russia on Ukraine

Threats observed or anticipated at time of reporting:

LinkedIn is an online professional networking site with a real identity requirement, which means that content posted by our members is visible to that member's professional network, including colleagues, managers, and potential future employers. As a result of LinkedIn's professional context, our members do not tend to post misinformation, nor does misinformation content gain traction on LinkedIn. Nonetheless, LinkedIn may be subject to certain members inadvertently posting misinformation during crisis situations.

Microsoft Advertising, in its role as an online advertising network, may be subject to the malicious use of its advertising services through either the spreading of misleading or deceptive advertising content or the funneling of advertising revenue to sites spreading disinformation.

Bing Search has observed instances of information manipulation with possible actor intent to manipulate search algorithms and lead users to data voids and low-authority content related to the Russia-Ukraine war. Themes included narratives involving Ukrainian immigrants in different countries, specific countries' support to Ukraine (often in the context of local elections) etc.

Mitigations in place at time of reporting:

Microsoft has been actively involved in identifying and helping counter Russia's cyber and influence operations aimed against Ukraine. In addition to supporting nonprofits, journalists, and academics within Ukraine, Microsoft's Threat Analysis Center (MTAC) team closely tracks cyber-enabled influence operations. MTAC analysts focused on Europe/Eurasia report on a wide range of Russian influence tactics used to malign or diminish support for Ukraine: propaganda and disinformation published across different languages; people-to-people and party-to-party engagement; real-world provocations; and those that blend cyber and influence activity, like hack-and-leak campaigns. MTAC's work includes analysing the ways these methods are leveraged to target audiences in Central and Eastern Europe.

In June of 2022, Microsoft issued its "[Defending Ukraine](#)" report and a follow up report issued in December 2022, both of which detailed the relentless and destructive Russian cyberattacks and influence operations, that we have directly observed in the hybrid war Russia is waging against Ukraine. Microsoft followed those reports with a report in March of 2023, outlining how Russia was regrouping for additional offensive measures against Ukraine including cyber and influence operations and a [report](#) in December of 2023 assessing Russian influence and cyber operations, including Russia's anti-Ukraine messaging to Israel and elsewhere. In February of 2024, Microsoft and OpenAI Issued a threat [report on activity by adversaries utilizing AI capability](#). This report identified recent Russian activity including activities targeting Ukraine.

LinkedIn's Professional Community Policies expressly prohibit false and misleading content, including [misinformation and disinformation](#), and its in-house Editorial team provides members with trustworthy content regarding global events, including the war in Ukraine. LinkedIn had approximately 1,443 content moderators globally (for 24/7 coverage), with 180 content moderators located in the EU as of 31 December 2024, and includes specialists in a number of languages including English, German, French, Russian, and Ukrainian. These reviewers use policies and guidance developed by a dedicated content policy team and experienced lawyers, and work with external fact checkers as

needed. When LinkedIn sees content or behaviour that violates its Professional Community Policies, it takes action, including the removal of content or the restriction of an account for repeated abusive behaviour. LinkedIn has been banned in Russia since 2016 and has implemented the European bans on Russian state media. In addition to not operating in Russia, political ads are banned on LinkedIn, which includes prohibitions on ads that exploit a sensitive political issue, including the current Russia-Ukraine war. LinkedIn also does not provide a mechanism for content creators to monetise the content they post on LinkedIn.

LinkedIn continues to mature its crisis response processes including 1) quickly coordinating with industry peers regarding the exchange of threat indicators; 2) engaging with external stakeholders regarding trends and TTPs; 3) continuously providing updated policy guidance to internal teams to assist with the removal of misinformation; and 4) continuing to proactively provide localised trustworthy information to our members.

LinkedIn has continued to mature its crisis response playbook by continually monitoring crisis situations globally, expanding internal teams that work on crisis response, and maturing our processes to respond more efficiently and effectively to crisis situations. LinkedIn will continue to follow its processes related to the removal of misinformation, and continually increase investments in resource allocation and process improvements where necessary to respond to the demands of the crisis.

Bing Search has implemented the following measures: (1) Defensive search interventions; (2) regular direction of users to high authority, high quality sources as part of search algorithms; (3) removed auto suggest and related search terms considered likely to lead users to low authority content as part of moderation; (4) authority demotion of identified nation state affiliated information manipulation actor domains and (5) partnerships with independent organizations to maintain threat intelligence and inform potential algorithmic interventions. These measures are also integrated into Bing generative AI experiences, along with the additional safeguards discussed at QRE 14.1.1 and QRE 14.1.2 and other measures discussed throughout this report.

[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].

Policies and Terms and Conditions

Outline any changes to your policies

Policy	Changes (such as newly introduced policies, edits, adaptation in scope or implementation)	Rationale
LinkedIn		

False or misleading content	LinkedIn continually updates its policies as appropriate during any crisis, including the Ukraine crisis.	Misinformation, disinformation campaigns, coordinated manipulative behaviours, malicious use of advertising products, and the involvement of foreign state actors, are all harms that existed prior to the Ukraine crisis, and therefore LinkedIn already had policies in place to address these harms.
Microsoft Advertising		
N/A	Microsoft Advertising has not implemented changes to its policies or introduced further measures specific to this crisis since the last reporting period.	No changes or new policies or measures were introduced due to the effectiveness of the measures already implemented. Microsoft Advertising is preventing serving advertising related to the Ukrainian crisis pursuant to its Sensitive Advertising Policies. Under this policy, Microsoft Advertising reserves the right to remove or limit advertising in response to a sensitive or high-profile news event to prevent the commercial exploitation of such events and to ensure user safety. Furthermore, our Misleading Content Policies prohibit advertising content that is misleading, deceptive, fraudulent, or that can be harmful to its users, including advertisements spreading disinformation. Microsoft Advertising requires its syndication partners (i.e., those partners that display our advertisements on their services) to abide by strict brand safety-oriented policies to avoid providing revenue streams to websites engaging in misleading, deceptive, harmful, or insensitive behaviours. Our publisher policies include a comprehensive list of prohibited content that ads cannot serve against, including, but not limited to, sensitive political content (e.g., extreme, aggressive, or misleading interpretations of news, events, or individuals), and unsavory content (such as content disparaging individuals or organisations). Partner properties that violate our policies are removed from our network until the partner remedies the issue. Microsoft Advertising banned all advertisements from the media outlets Russia Today (RT) and Sputnik across our ad network and will not place any ads from our ad network on these sites.
Bing Search		
N/A	Bing has not implemented additional policies specific to this crisis since its last report.	Prior to this reporting period, Bing had already established measures to address this crisis. Although Bing continues to refine its approach to addressing this crisis

		and continues to evolve mitigation measures, it has not introduced specific policy changes this reporting period.
Scrutiny of Ads Placements		
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.		
LinkedIn		
Specific Action applied (with reference to the Code’s relevant Commitment and Measure)	Description of intervention Political ads are banned on LinkedIn, which includes prohibitions on ads that exploit a sensitive political issue. LinkedIn does not pay its members for creating content, other than in rare instances where we individually select and manage a small group of content creators to create professionally relevant content.	
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available n/a	
Microsoft Advertising		
Specific Action applied (with reference to the Code’s relevant Commitment and Measure)	Description of intervention Microsoft Advertising is preventing serving advertising related to the War of aggression by Russia on Ukraine pursuant to its Sensitive Advertising Policies. Under this policy, Microsoft Advertising reserves the right to remove or limit advertising in response to a sensitive or high-profile news event to prevent the commercial exploitation of such events and to ensure user safety. Furthermore, our Misleading Content Policies prohibit advertising content that is misleading, deceptive, fraudulent, or that can be harmful to its users, including advertisements spreading disinformation. Microsoft Advertising requires its syndication partners (i.e., those partners that display our advertisements on their services) to abide by strict brand safety-oriented policies to avoid providing revenue streams to websites engaging in misleading, deceptive, harmful, or insensitive behaviours. Our publisher policies include a comprehensive list of prohibited content that ads cannot serve against, including, but not limited to, sensitive political content (e.g., extreme, aggressive, or misleading interpretations of news, events, or individuals), and unsavory content (such as content disparaging individuals or organisations). Partner properties that violate our policies are removed from our network until the partner remedies the issue.	

	<p>As stated in our revised policies, “We may use a combination of internal signals and trusted third-party data or information sources to reject, block, or take down ads or sites that contain disinformation or send traffic to pages containing disinformation.”</p> <p>Microsoft Advertising partners with third parties as sources for strategic intelligence on domains. Microsoft Advertising actions domains, based in part on these sources evaluations as foreign influence related or non-compliant.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>During the relevant reporting period, Microsoft Advertising blocked no additional search queries, leaving the total of search queries blocked at 736, and blocked no additional web domains across its network, leaving the total of domains blocked at 2,789.</p> <p>Microsoft Advertising maintained the suspension placed on all 1,483 existing Russian-based advertisers prior to the relevant reporting period and did not acquire any new Russian-based advertisers during the relevant reporting period.</p>
Political Advertising	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	
Specific Action applied (with reference to the Code’s relevant Commitment and Measure)	<p>Description of intervention</p> <p>Not applicable. Political ads are banned on LinkedIn, which includes prohibitions on ads that exploit a sensitive political issue.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>n/a</p>
Microsoft Advertising	
Specific Action applied (with reference to the Code’s relevant Commitment and Measure)	<p>Description of intervention</p> <p>Not applicable. As described in Section 3 of the report, Microsoft Advertising does not support political advertising.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>n/a</p>

Integrity of Services	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention LinkedIn's Professional Community Policies prohibit misinformation, and misinformation is removed from the LinkedIn platform. Members that post misinformation are notified of LinkedIn's removal of their content. Members that repeatedly post misinformation are permanently restricted. State-sponsored attempts to post misinformation, if any, are removed. LinkedIn also maintains a robust ad-review process to prevent malicious advertising wherein ads related to crises, including the Ukraine war, are manually reviewed and approved by our internal team. LinkedIn regularly meets with and exchanges information with industry peers to identify and share granular information related to manipulative behaviours, coordinated influence operations, and TTPs. All such content that violates LinkedIn's Professional Community Policies is removed.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available LinkedIn does not track misinformation content removal by subject matter, and a comprehensive listing of its misinformation content takedowns is provided in this disclosure and in its Transparency Report. See also SLI 18.2.1. Impact metrics for malicious advertising removals are available in SLI 2.1.1 and 2.3.1, whereas metrics related to manipulative behaviors and TTPs are available in SLI 12.1.1 and 14.2.1.
Bing Search	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention Bing Search has implemented the following measures: (1) Defensive search interventions; (2) regular direction of users to high authority, high quality sources as part of search algorithms; (3) removed auto suggest and related search terms considered likely to lead users to low authority content as part of moderation; (4) authority demotion of identified nation state affiliated information manipulation actor domains and (5) partnerships with independent organizations for threat intelligence to inform potential algorithmic interventions.

	These measures are also integrated into Bing generative AI features, along with the additional safeguards discussed at QRE 14.1.1 and QRE 14.1.2 and other measures discussed throughout this report.
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>Globally, more than 798,637 queries searched by users related to the Russia-Ukraine war have been treated with defensive search interventions, resulting in over 18.1 million impressions. In the EEA, this resulted in 1,731,889 impressions. For member state level reporting, see SLI 22.7.1.</p>
Empowering Users	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>LinkedIn has an internal team of global news editors that provides trustworthy and authoritative content to its member-base at all times. During important events in the Ukraine crisis, this team provides manually curated and localised storylines.</p>
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available
Bing Search	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>Articles from news and fact checking organizations may also appear as part of specialized Bing Answers. In addition, news and fact-check articles can appear in Bing News carousels, which are often presented at the top of search results pages, depending on the nature of user query. Microsoft maintains agreements with news publishers to surface high authority content, including articles from well-regarded fact checking organizations and journalist-driven fact-checks, high in relevant search results.</p> <p>In addition, Bing uses threat intelligence to inform the Bing algorithm and defensive search measures used for Bing search and Bing's generative search features. Bing works with trusted third-party partners for leads of potential threats (including in EEA member state</p>

	<p>territories and languages) to inform defensive search strategies for Bing. Bing also utilises the ClaimReview open protocol to ingest fact checks into search results.</p> <p>Bing has increased coverage of EEA languages, informing interventions across monitored themes and sources.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>See QRE 22.7.1 and QRE 21.1.1 for further information.</p>
Empowering the Research Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>None for LinkedIn</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>None for LinkedIn</p>
Bing Search	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>See QRE 26.1.1 for general research support. Bing Search has not made datasets available pertaining specifically to this crisis.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>n/a</p>
Microsoft	
	Description of intervention:

Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Microsoft has provided funding to Report for the World to support reporting positions with trustworthy newsrooms in Ukraine, including Kyiv Independent, ABO, Hromadske and has also invested in the expansion of the Kyiv Independent's War Crimes Investigative Unit to allow for more in-depth reporting. This allows for leveraging authoritative sources of information in the region including by adding the Kyiv Independent our Start platform.</p> <p>Microsoft published analysis from its Microsoft Threat Analysis Center on how Russian US election interference targets support for Ukraine in April 2024. This election report provides an update on what Microsoft has observed from Russia, Iran, and China and malicious use of AI since our November 2023 report.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>n/a</p>
Empowering the Fact-Checking Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>LinkedIn works with globally-recognised factcheckers to receive their independent judgment regarding user-generated content. Content that violates LinkedIn's policy on false and misleading content is removed.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>LinkedIn does not separately track Ukraine related content sent to external fact checkers. Further detail regarding content sent to fact checkers is available at SLI 21.1.1, 30.1.1, and 31.1.1.</p>
Bing Search	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>Articles from news and fact-checking organizations may appear as part of specialized Bing Answers. In addition, news and fact-check articles can appear in Bing News carousels, which are often presented at the top of search results pages, depending on the nature of</p>

	<p>user query. Microsoft maintains agreements with news publishers to surface high authority content, including articles from well-regarded fact checking organizations and journalist-driven fact-checks, high in relevant search results.</p> <p>In addition, Bing utilizes threat intelligence to inform the Bing algorithm and defensive search measures for Bing search and Bing generative AI features. Bing works with trusted third-party partners for early indicators of potential threats (including in EEA member state languages) that can be leveraged to inform defensive search strategies. Bing also utilises the ClaimReview open protocol to ingest fact checks into search results.</p> <p>Bing has increased the coverage of EEA member state languages, informing interventions across monitored themes and sources. Generative AI features in Bing are subject to Microsoft's robust safety classifiers (which are informed by data shared by information integrity partners and other authority signals) to prevent the creation of low authority materials or misinformation.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available n/a</p>
--	--

Reporting on the services' response during a crisis

Israel-Hamas Conflict

Threats observed or anticipated at time of reporting:

LinkedIn is an online professional networking site with a real identity requirement, which means that content posted by our members is visible to that member's professional network, including colleagues, managers, and potential future employers. As a result of LinkedIn's professional context, our members come to LinkedIn for economic opportunity, and as such, do not tend to post misinformation, nor does misinformation content gain traction on LinkedIn. Nonetheless, LinkedIn may be subject to certain members inadvertently posting misinformation during crisis situations.

Bing Search has observed instances of data void manipulation to show low-authority content to unsuspecting users related to the Israel-Hamas conflict. This type of search algorithm manipulation could potentially be used as a tactic to spread disinformation. Other themes observed have included foreign influence operations speculating on the evolution of conflict in the area; alleged relations between Ukraine and Hamas; and information manipulation on military operations or the impact of the conflict.

Mitigations in place at time of reporting:

LinkedIn's Professional Community Policies expressly prohibit false and misleading content, including [misinformation and disinformation](#), and its in-house Editorial team provides members with trustworthy content regarding global events, including the Israel-Hamas conflict. LinkedIn had approximately 1,443 content moderators globally (for 24/7 coverage), with 180 content moderators located in the EU as at 31 December 2024, and includes specialists in languages supported on LinkedIn. These reviewers use policies and guidance developed by a dedicated content policy team and experienced lawyers, and work with external fact checkers as needed. When LinkedIn sees content or behaviour that violates its Professional Community Policies, it takes action, including the removal of content or the restriction of an account for repeated abusive behaviour. Political ads are banned on LinkedIn, which includes prohibitions on ads that exploit a sensitive political issue, including the current Israel-Hamas conflict. LinkedIn also does not provide a mechanism for content creators to monetise the content they post on LinkedIn.

LinkedIn continues to mature its crisis response processes including 1) quickly coordinating with industry peers regarding the exchange of threat indicators; 2) engaging with external stakeholders regarding trends and TTPs; 3) continuously providing updated policy guidance to internal teams to assist with the removal of misinformation; and 4) continuing to proactively provide localised trustworthy information to our members.

LinkedIn has continued to mature its crisis response playbook by continually monitoring crisis situations globally, expanding internal teams that work on crisis response, and maturing our processes to respond more efficiently and effectively to crisis situations. LinkedIn will continue to follow its processes related to the removal of misinformation, and continually increase investments in resource allocation and process improvements where necessary to respond to the demands of the crisis.

Bing Search: As part of its regular practices, Bing search employs (1) Defensive search interventions; (2) regular direction of users to high authority, high quality sources as part of search algorithms; (3) removal of auto suggest and related search terms considered likely to lead users to low authority content as part of moderation; (4) authority demotion

of identified nation state affiliated information manipulation actor domains; and (5) partnerships with independent organizations for threat intelligence to inform potential algorithmic interventions. These measures are also integrated into Bing generative AI features, along with the additional safeguards discussed at QRE 14.1.1 and QRE 14.1.2 and other measures discussed throughout this report.

[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].

Policies and Terms and Conditions

Outline any changes to your policies

Policy	Changes (such as newly introduced policies, edits, adaptation in scope or implementation)	Rationale
LinkedIn		
False or misleading content	LinkedIn continually updates its policies as appropriate during any crisis, including the Israel-Hamas conflict.	Misinformation, disinformation campaigns, coordinated manipulative behaviours, malicious use of advertising products, and the involvement of foreign state actors, are all harms that existed prior to the Israel-Hamas conflict, and therefore LinkedIn already had policies in place to address these harms.

Microsoft Advertising

Microsoft Advertising has not introduced specific policies related to this crisis, as it considers existing measures discussed throughout this report to sufficiently mitigate risks related to this crisis.

Bing Search

Bing Search has not introduced specific policies related to this crisis, as it considers existing measures discussed throughout this report to sufficiently mitigate risks related to this crisis.

Scrutiny of Ads Placements

Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>Political ads are banned on LinkedIn, which includes prohibitions on ads that exploit a sensitive political issue, including the current Israel-Hamas conflict. LinkedIn also does not provide a mechanism for content creators to monetise the content they post on LinkedIn.</p> <p>LinkedIn does not pay its members for creating content, other than in rare instances where we individually select and manage a small group of content creators to create professionally relevant content.</p>
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available
Microsoft Advertising	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>Microsoft Advertising is preventing serving advertising related to the Israel-Hamas conflict pursuant to its Sensitive Advertising Policies. Under this policy, Microsoft Advertising reserves the right to remove or limit advertising in response to a sensitive or high-profile news event to prevent the commercial exploitation of such events and to ensure user safety. Furthermore, our Misleading Content Policies prohibit advertising content that is misleading, deceptive, fraudulent, or that can be harmful to its users, including advertisements spreading disinformation. Microsoft Advertising requires its syndication partners (i.e., those partners that display our advertisements on their services) to abide by strict brand safety-oriented policies to avoid providing revenue streams to websites engaging in misleading, deceptive, harmful, or insensitive behaviours. Our publisher policies include a comprehensive list of prohibited content that ads cannot serve against, including, but not limited to, sensitive political content (e.g., extreme, aggressive, or misleading interpretations of news, events, or individuals), and unsavory content (such as content disparaging individuals or organisations). Partner properties that violate our policies are removed from our network until the partner remedies the issue.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>During the relevant reporting period, Microsoft Advertising blocked any ads on 36 search queries and blocked 3 web domains across its network.</p>
Political Advertising	

Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention Not applicable. Political ads are banned on LinkedIn, which includes prohibitions on ads that exploit a sensitive political issue, including the current Israel-Hamas conflict.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available n/a
Microsoft Advertising	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention Not applicable. As described in Section 3 of the report, Microsoft Advertising does not support political advertising.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available n/a
Integrity of Services	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention LinkedIn's Professional Community Policies prohibit misinformation, and misinformation is removed from the LinkedIn platform. Members that post misinformation are notified of LinkedIn's removal of their content. Members that repeatedly post misinformation are permanently restricted. State-sponsored attempts to post misinformation, if any, are removed.

	<p>LinkedIn also maintains a robust ad-review process to prevent malicious advertising wherein ads related to crises, including the Israel-Hamas conflict, are manually reviewed and approved by our internal team.</p> <p>LinkedIn regularly meets with and exchanges information with industry peers to identify and share granular information related to manipulative behaviours, coordinated influence operations, and TTPs. All such content that violates LinkedIn's Professional Community Policies is removed.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>Impact metrics for malicious advertising removals are available in SLI 2.1.1 and 2.3.1, whereas metrics related to manipulative behaviors and TTPs are available in SLI 12.1.1 and 14.2.1.</p>
Bing Search	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>Bing Search has not introduced specific practices or policies related to this crisis, as it considers existing measures discussed throughout this report to sufficiently mitigate risks. However, Bing continues to monitor this crisis and may evolve its approach as needed.</p> <p>As part of its regular practices, Bing Search employs (1) Defensive search interventions; (2) regular direction of users to high authority, high quality sources as part of search algorithms; (3) removal of auto suggest and related search terms considered likely to lead users to low authority content as part of moderation; (4) authority demotion of identified nation state affiliated information manipulation actor domains; and (5) partnerships with independent organizations for threat intelligence to inform potential algorithmic interventions. These measures are also integrated into Bing generative AI features, along with the additional safeguards discussed at QRE 14.1.1 and QRE 14.1.2 and other measures discussed throughout this report.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>n/a</p>
Empowering Users	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	
Specific Action applied (with reference to the	<p>Description of intervention</p>

Code's relevant Commitment and Measure)	LinkedIn has an internal team of global news editors that provides trustworthy and authoritative content to its member-base at all times. During important events in the Israel-Hamas conflict, this team provides manually curated and localised storylines.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available
Bing Search	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>Bing Search has not introduced specific practices or policies related to this crisis, as it considers existing measures discussed throughout this report to sufficiently mitigate risks. However, Bing continues to monitor this crisis and may evolve its approach as needed.</p> <p>Nonetheless, articles from news and fact checking organizations may also appear as part of specialized Bing Answers. In addition, news and fact-check articles can appear in Bing News carousels, which are often presented at the top of search results pages, depending on the nature of user query. Microsoft maintains agreements with news publishers to surface high authority content, including articles from well-regarded fact checking organizations and journalist-driven fact-checks, high in relevant search results.</p> <p>In addition, Bing utilizes a number of threat intelligence to inform the Bing algorithm and defensive search measures for Bing search and Bing generative AI features. Bing works with trusted third-party partners for leads of potential threats (including in EEA member state languages) that can be leveraged to inform defensive search strategies for Bing. Bing also utilises the ClaimReview open protocol to ingest fact checks into search results.</p> <p>Bing increased the coverage of EEA member state languages informing interventions across monitored themes and sources.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>n/a</p>
Empowering the Research Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	
Specific Action applied (with reference to the	Description of intervention

Code's relevant Commitment and Measure)	None for LinkedIn
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available None for LinkedIn
Bing Search	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention See QRE 26.1.1 for general research support. Bing Search has not made datasets available pertaining specifically to this crisis.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available
Empowering the Fact-Checking Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention LinkedIn works with globally-recognised factcheckers to receive their independent judgment regarding user-generated content. Content that violates LinkedIn's policy on false and misleading content is removed.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available LinkedIn does not separately track Israel-Hamas conflict related content sent to external fact checkers. Further detail regarding content sent to fact checkers is available at SLI 21.1.1, 30.1.1, and 31.1.1.
Bing Search	
Specific Action applied (with reference to the	Description of intervention

Code's relevant Commitment and Measure)	<p>Bing utilizes threat intelligence to inform the Bing algorithm and defensive search measures for Bing search and Bing generative AI features. Bing works with trusted third-party partners for leads of potential threats (including in EEA member state languages) to inform defensive search strategies for Bing. Bing also utilises the ClaimReview open protocol to ingest fact checks into search results.</p> <p>Bing has increased the overall volume of EEA language coverage, informing interventions across monitored themes and sources.</p> <p>Generative AI features in Bing are subject to Microsoft's robust safety classifiers (which are informed by data shared by information integrity partners and other authority signals) to prevent the creation of low authority materials or misinformation.</p>
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available
Microsoft	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>Microsoft continues to grow partnerships to strengthen the company's capacity and ability to combat information operations globally.</p>
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available

Reporting on the services' response during an election

Reporting on the services' response during an election

2024 French Parliamentary Elections

Threats observed during the electoral period:

LinkedIn is an online professional networking site with a real identity requirement, which means that content posted by our members is visible to that member's professional network, including colleagues, managers, and potential future employers. As a result of LinkedIn's professional context, our members come to LinkedIn for economic opportunity, and as such, do not tend to post misinformation, nor does misinformation content gain traction on LinkedIn. Nonetheless, LinkedIn may be subject to certain members inadvertently posting misinformation during elections.

Bing Search anticipated instances of information manipulation with possible actor intent to manipulate search algorithms and lead users to data voids and low-authority content related to elections. As part of its regular information integrity operations, Bing detected information manipulation themes related to the 2024 French Parliamentary Election, which have been ingested to inform defensive search interventions, along with special How to Vote answer implemented pointing to authoritative sources.

Mitigations in place during the electoral period:

LinkedIn's Professional Community Policies expressly prohibit false and misleading content, including [misinformation and disinformation](#), and its in-house Editorial team provides members with trustworthy content regarding global events, including French elections. LinkedIn had approximately 1,443 content moderators globally (for 24/7) coverage, with 180 content moderators located in the EU as at 31 December 2024, and includes specialists in a number of languages including French. These reviewers use policies and guidance developed by a dedicated content policy team and experienced lawyers, and work with external fact checkers as needed. When LinkedIn sees content or behaviour that violates its Professional Community Policies, it takes action, including the removal of content or the restriction of an account for repeated abusive behaviour.

Political ads are banned on LinkedIn, which includes prohibitions on ads that exploit a sensitive political issue, including European Elections. LinkedIn also does not provide a mechanism for content creators to monetise the content they post on LinkedIn.

LinkedIn continues to mature its crisis response processes. In addition to the increase in resource allocation and process improvements, best practices include: 1) quickly coordinating with industry peers regarding the exchange of threat indicators; 2) engaging with external stakeholders regarding trends and TTPs; 3) continuously providing updated policy guidance to internal teams to assist with the removal of misinformation; and 4) continuing to proactively provide localised trustworthy information to our members.

LinkedIn has continued to mature its crisis response playbook by continually monitoring crisis situations globally, expanding internal teams that work on crisis response, and maturing our processes to respond more efficiently and effectively to crisis situations. LinkedIn will continue to follow its processes related to the removal of misinformation, and continually increase investments in resource allocation and process improvements where necessary to respond to the demands of the crisis.

LinkedIn also implemented a specialized intake and operations process under the Elections Working Group Rapid Response System for the French Parliamentary elections.

Bing Search takes a multifaceted approach to protecting election integrity and regularly updates its processes, policies, and practices to adapt to evolving risks, trends, and technological innovations. This approach includes: (1) defensive search interventions; (2) regular direction of users to high authority, high quality sources; (3) removal of auto suggest and related search terms considered likely to lead users to low authority content; (4) partnerships with independent organisations for threat intelligence on information manipulation, civic integrity and nation state affiliated actors to inform potential algorithmic interventions and contribute to broader research community; (5) special information panels and answers to direct users to high authority sources concerning elections and voting; (6) internal working groups dedicated to addressing company-wide election initiatives; (7) establishing special election-focused product feature teams; (8) conducting internal research on content provenance and elections; (9) evaluating and undertaking red-team testing for generative AI features with respect to elections ; (10) ensuring Responsible AI reviews for all AI features; (11) undertaking comprehensive risk assessments related to elections and electoral processes; (12) developing and continuing to improve targeted monitoring both for web search and Bing generative AI experiences; (13) restricting generative responses for certain types of election-related content; (14) leveraging blocklists and classifiers in Bing generative AI experiences to restrict generation of images or certain types of content concerning political candidates and certain election-related topics (15) integrating information on political parties, candidates, and elections from local election authorities (including in the EU) or high authority third party sources to inform defensive interventions and election-related product mitigations; and (16) regularly evaluating whether additional measures, metrics, or mitigations should be implemented. These measures are integrated into Bing Search and Bing generative AI experiences, along with the additional safeguards discussed at QRE 14.1.1 and QRE 14.1.2 and other measures discussed throughout this report.

Bing also maintains an incident response process for cross-functional teams to prioritize high-risk incidents and track the investigation, fixes, and post-incident analysis. Internal escalation processes are set up to ensure urgent cases— including sensitive issues related to elections or election-related content -- are addressed expediently with high priority. Bing also implemented a specialized intake and operations process under the Elections Working Group Rapid Response System and coordinates with Democracy Forward Election Hubs on incidents.

Bing also undertakes internal post-election reviews, as appropriate, to evaluate product and mitigation performance, reflect on challenges and learnings, and identify potential areas for improvement. These reviews occur both in product review settings and in broader cross-functional teams dedicated to elections at Microsoft.

Microsoft's Democracy Forward team continues to expand its collaborations with organizations that provide information on authoritative sources, ensuring that queries about global events will surface reputable sites.

While not announced during the current reporting period, it is worth mentioning that in February 2024, Microsoft and LinkedIn came together with the tech sector at the Munich Security Conference to take a vital step forward against AI deepfakes, which will make it more difficult for malicious threat actors to use legitimate tools to create deepfakes. This focuses on the work of companies that create content generation tools and calls on them to strengthen the safety architecture in AI services by assessing risks and strengthening controls to help prevent abuse. This includes aspects such as ongoing red team analysis, preemptive classifiers, the blocking of abusive prompts, automated testing, and rapid bans of users who abuse the system. The accord brings the tech sector together to detect and respond to deepfakes in elections and will help advance transparency and build societal resilience to deepfakes in elections.

We combined this work with the launch of an expanded Digital Safety Unit. This will extend the work of our existing digital safety team, which has long addressed abusive online content and conduct that impacts children or that promotes extremist violence, among other categories. This team has special ability in responding on a 24/7 basis to

weaponized content from mass shootings that we act immediately to remove from our services. The accord's commitments oblige Microsoft and the tech sector to continue to engage with a diverse set of global civil society organizations, academics, and other subject matter experts. These groups and individuals play an indispensable role in the promotion and protection of the world's democracies.

See more at [Microsoft announces new steps to help protect elections - Microsoft On the Issues and Meeting the moment: combating AI deepfakes in elections through today's new tech accord - Microsoft On the Issues.](#)

In advance of the EU elections this summer we kicked off a global effort to engage campaigns and elections authorities to deepen understanding of the possible risks of deceptive AI in elections and empower those campaigns and election officials to speak directly to their voters about these risks steps they can take to build resilience and increase confidence in the election. In 2024, we have conducted nearly 200 training sessions for political stakeholders in 25 countries, reaching over 4300 participants. This includes almost 50 separate training events with over 500 participants across EEA, including in France prior to the parliamentary elections.

As part of Microsoft's commitments related to public awareness and engagement, Microsoft ran a campaign titled [Check. Recheck. Vote.](#) containing a series of public messages and stood up an AI and Elections website focused on engaging voters about the risks of deceptive AI and where to find authoritative election information. This campaign ran across the EU, France, UK, and the US in the lead up to major elections. Globally, the campaign reached hundreds of millions of people, with millions interacting with the content, connecting them with official election information.

In addition, Microsoft is harnessing the data science and technical capabilities of our AI for Good Lab and MTAC teams to better assess whether abusive content—including that created and disseminated by foreign actors—is synthetic or not. Microsoft AI for Good Lab has been developing detection models (image, video) to assess whether media was generated or manipulated by AI. The model is trained on approximately 200,000 examples of AI and real content. AI for Good continues to invest in creating sample dataset representing the latest generative AI technology. When appropriate, we call on the expertise of Microsoft's Digital Crimes Unit to invest in and operationalize the early detection of AI-powered criminal activity and respond appropriately, through the filing of affirmative civil actions to disrupt and deter that activity and through threat intelligence programs and data sharing with customers and government.

We are also empowering candidates, campaigns and election authorities to help us detect and respond to deceptive AI targeting elections. In February 2024, we launched the Microsoft-2024 Elections site where candidates in a national or federal election can directly report deceptive AI election content on Microsoft consumer services. This reporting tool allows for 24/7 reporting by impacted election entities who have been targeted by deceptive AI found on Microsoft platforms.

[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].

Policies and Terms and Conditions

Outline any changes to your policies		
Policy	Changes (such as newly introduced policies, edits, adaptation in scope or implementation)	Rationale
Bing Search		
Authoritative Information sources	In advance of French Parliamentary elections, Bing launched special “How to Vote” Answer segments to show high authority information related to the election for users in France, localized by language. Bing Search directed users to official sources from the Ministry of Interior on section information seeking queries related to this election.	See more at Microsoft announces new steps to help protect elections - Microsoft On the Issues and the location specific blogs below. France: Microsoft is committed to preserving the sincerity of the legislative elections in France
Microsoft		
Deepfakes and Elections	Last year Microsoft launched a web page – Microsoft-2024 Elections – where political candidates can report alleged deepfakes of themselves to Microsoft. To date, we have not received an actionable report of deceptive AI targeting elections on Microsoft platforms. Microsoft’s Office of Responsible AI has also established policies concerning election-related content and works with teams, including Bing and Image Creator on implementation.	See more at Meeting the moment: combating AI deepfakes in elections through new tech accord
Content Integrity tools	During the reporting period, Microsoft continued piloting Content Integrity Tools, which allowed users to add content credentials to their own authentic content. Designed as a pilot program primarily to support the 2024 election cycle and gather feedback about Content Credentials-enabled tools, during the reporting period of this report, the tools were available to political campaigns in the EU, as well as to elections authorities and select news media organizations in the EU and globally. These tools included a partnership and collaboration	These watermarking credentials empower an individual or organization to assert that an image or video came from them while protecting against tampering by showing if content was altered after its credentials were created. See more at Expanding our Content Integrity tools to support global elections - Microsoft On the Issues

	with fellow Tech Accord signatory, TruePic. Announced in April 2024, this collaboration leveraged TruePic's mobile camera SDK enabling campaign, election, and media participants to capture authentic images, videos and audio directly from a vetted and secure device. Called the "Content Integrity Capture App" (an app that makes it easy to directly capture images with C2PA enabled signing) launched for both Android and Apple and can be used by participants in the Content Integrity Tools pilot program.	
Campaign Success Teams	Microsoft helps political campaigns navigate cybersecurity challenges and the new world of AI by deploying a newly formed "Campaign Success Team" within Microsoft Philanthropies' Tech for Social Impact organization. This team advises and supports campaigns as they navigate the world of AI, combat the spread of cyber influence campaigns, and protect the authenticity of their own content and images.	See more at Microsoft announces new steps to help protect elections - Microsoft On the Issues
AI Elections Trainings	As part of our commitments related to public awareness and engagement, Microsoft ran a campaign titled Check. Recheck. Vote. containing a series of public messages and stood up an AI and Elections website focused on engaging voters about the risks of deceptive AI and where to find authoritative election information. This campaign ran across the EU, UK, and the US in the lead up to major elections. Globally, the campaign reached hundreds of millions of people, with millions interacting with the content, connecting them with official election information.	
Communications Hub	Microsoft created and provides access to an "Election Communications Hub" to support democratic governments around the world as they build secure and resilient election processes.	See more at Microsoft announces new steps to help protect elections - Microsoft On the Issues


Virtual Situation Room	Microsoft established a Virtual Situation Room, bringing together resources across the company to monitor, support, and protect the French elections. This situation room tied into the rapid response protocol under the DSA. While Microsoft did not receive any reporting through the rapid response protocol throughout the French election we were prepared to intake any reporting and quickly respond.	
Foreign Malign Influence Updates	<p>Microsoft publishes regular reports on foreign malign influence researched and reported by the company's MTAC team. The first report was released in November 2023.</p> <p>Microsoft also published MTAC analysis on how Russian US election interference targets support for Ukraine in April 2024. This election report provides an update on what Microsoft has observed from Russia, Iran, and China and malicious use of AI since our November 2023 report.</p>	<p>See more at Microsoft announces new steps to help protect elections - Microsoft On the Issues</p> <p>See more at Meeting the moment: combating AI deepfakes in elections through new tech accord</p> <p>See more at Russian US election interference targets support for Ukraine after slow start - Microsoft On the Issues</p>
LinkedIn		
False or misleading content	LinkedIn continually updates its policies as appropriate during any major global event, including French elections.	Misinformation, disinformation campaigns, coordinated manipulative behaviours, malicious use of advertising products, and the involvement of foreign state actors, are all harms that existed prior to the French elections, and therefore LinkedIn already had policies in place to address these harms.
Scrutiny of Ads Placements		
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.		
LinkedIn		

Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>Political ads are banned on LinkedIn, which includes prohibitions on ads that exploit a sensitive political issue, including Frenchelections.</p> <p>LinkedIn does not pay its members for creating content, other than in rare instances where we individually select and manage a small group of content creators to create professionally-relevant content.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>n/a</p>
Microsoft Advertising	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>As described in Section 3 of the report, Microsoft Advertising does not support political advertising.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>During the relevant reporting period, Microsoft Advertising blocked 191 phrases, which prevented keyword or ad submissions for the French election candidates and parties.</p>
Political Advertising	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	
Specific Action applied (with reference to the	<p>Description of intervention</p> <p>Political ads are banned on LinkedIn, which includes prohibitions on ads that exploit a sensitive political issue, including European elections.</p>

Code's relevant Commitment and Measure)	
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available n/a
Microsoft Advertising	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention Not applicable. As described in Section 3 of the report, Microsoft Advertising does not support political advertising.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available n/a
Integrity of Services	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention LinkedIn also maintains a robust automated and manual ad-review process to prevent ads related to European Elections from running on our platform. LinkedIn regularly meets with and exchanges information with industry peers to identify and share granular information related to manipulative behaviours, coordinated influence operations, and TTPs. All such content that violates LinkedIn's Professional Community Policies is removed.

	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>LinkedIn does not track misinformation content removal by subject matter, and a comprehensive listing of its misinformation content takedowns is provided in this disclosure and in its Transparency Report. See also SLI 18.2.1.</p> <p>Impact metrics for malicious advertising removals are available in SLI 2.1.1 and 2.3.1, whereas metrics related to manipulative behaviors and TTPs are available in SLI 12.1.1 and 14.2.1.</p>
Bing Search	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>Bing Search takes a multifaceted approach to protecting election integrity and regularly updates its processes, policies, and practices to adapt to evolving risks, trends, and technological innovations. This approach includes: (1) defensive search interventions; (2) regular direction of users to high authority, high quality sources; (3) removal of auto suggest and related search terms considered likely to lead users to low authority content; (4) partnerships with independent organizations for threat intelligence on information manipulation, civic integrity and nation state affiliated actors to inform potential algorithmic interventions and contribute to broader research community; (5) special information panels and answers to direct users to high authority sources concerning elections and voting; (6) internal working groups dedicated to addressing company-wide election initiatives; (7) establishing special election-focused product feature teams; (8) conducting internal research on content provenance and elections; (9) evaluating and undertaking red-team testing for generative AI features with respect to elections; (10) ensuring Responsible AI reviews for all AI features; (11) undertaking comprehensive risk assessments related to elections and electoral processes; (12) developing and continuing to improve targeted monitoring both for web search and generative AI features; (13) restricting responses for certain types of election-related content; (14) leveraging blocklists and classifiers in Bing generative AI experiences to restrict generation of images or certain types of content concerning political candidates and certain election-related topics (15) integrating information on political parties, candidates, and elections from local election authorities (including in the EU) or high authority third party sources to inform defensive interventions and election-related product mitigations; and (16) regularly evaluating whether additional measures, metrics, or mitigations should be implemented. These measures are integrated into Bing Search and Bing generative AI experiences, along with the additional safeguards discussed at QRE 14.1.1 and QRE 14.1.2 and other measures discussed throughout this report.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <ul style="list-style-type: none"> • In advance of the France parliamentary election, Bing launched a special "How to Vote" information Answer to show high authority information related to the election for users in France., localized by language. Bing Search directed users to official sources from the Ministry of Interior on select information seeking queries related to this election. This has led to 36k total impressions. • Bing has identified numerous information manipulation themes related to the 2024 French Parliamentary election, which have informed defensive search interventions and fanouts to related search terms.

Empowering Users	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>LinkedIn has an internal team of global news editors that provides trustworthy and authoritative content to its member-base at all times. During important events in European elections, this team provides manually curated and localised storylines.</p>
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available
Bing Search	
Partnerships with Election Authorities and Trusted Partners (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>Bing Search empowers voters with authoritative election information on Bing. We do this in partnership with organizations that provide information on authoritative sources, ensuring that queries about election administration will surface reputable sites.</p>
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available

<p>Specific Action applied (with reference to the Code's relevant Commitment and Measure)</p>	<p>Description of intervention</p> <p>In advance of the France parliamentary election, Bing launched a special “How to Vote” information Answer to show high authority information related to the election for users in France, localized by language. Bing Search directed users to official source from the Ministry of Interior on select information seeking queries related to this election, as depicted below.</p> 
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p><u>How to Vote Answers</u></p> <p>Bing documented 36,000 impressions globally on the “How to Vote” special answer for the France parliamentary election in the answer implementation period from 21 June – 8 July 2024, out of which 14,800 occurred in the reporting period (after 1 July 2024)</p>
<p>Empowering the Research Community</p>	

Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Bing Search	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>None for Bing</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>Such research helps to inform Bing safety mitigations.</p>
LinkedIn	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>None for LinkedIn</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>None for LinkedIn</p>
Empowering the Fact-Checking Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	

Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>LinkedIn works with globally-recognised factcheckers to receive their independent judgment regarding user-generated content. Content that violates LinkedIn's policy on false and misleading content is removed.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>LinkedIn does not separately track election related content sent to external fact checkers. Further detail regarding content sent to fact checkers is available at SLI 21.1.1, 30.1.1, and 31.1.1.</p>
Bing Search	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>Bing utilizes threat intelligence to inform the Bing algorithm and defensive search measures for Bing search and Bing generative AI features. Bing works with trusted third-party partners for leads of potential threats (including in EEA member state languages) to inform defensive search strategies. Bing also utilises the ClaimReview open protocol to ingest fact checks into search results.</p> <p>Bing increased coverage of EEA member state languages, informing interventions across monitored themes and sources.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>n/a</p>
Microsoft	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>In December 2023, the Institute for Nonprofit News teamed up with DeleteMe, funded by Microsoft's Democracy Forward Initiative, to help decrease the amount of personal information about journalists that can be discovered online. The collaboration protects local journalists from threats during a critical election year and ensures they can provide high-quality information to local communities. The Microsoft Journalism Hub is an ongoing resource center built to connect the journalism community more seamlessly with tools, technology, services, and partner programs designed to support their unique</p>

	<p>business needs. These resources are distributed across Microsoft’s three journalism initiative commitments: rebuilding capacity in local news ecosystems; restoring trust in news; and reducing legal and cyber risks for journalists.</p> <p>Microsoft has partnered with Nota to allow journalists to access helpful AI tools for tasks such as improving SEO, creating videos of published stories, and writing headlines. Nota’s assistive AI tools build time-saving production infrastructure for digital publishing—creating an accessible engagement economy, offering instant content conversion and content amplification, multiplying video content revenue and doing away with repetitive tasks that have long required journalists to act as generalists in multiple fields.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>n/a</p>

Reporting on the services' response during an election

2024 Romanian Presidential Elections

Threats observed during the electoral period:

LinkedIn is an online professional networking site with a real identity requirement, which means that content posted by our members is visible to that member's professional network, including colleagues, managers, and potential future employers. As a result of LinkedIn's professional context, our members come to LinkedIn for economic opportunity, and as such, do not tend to post misinformation, nor does misinformation content gain traction on LinkedIn. Nonetheless, LinkedIn may be subject to certain members inadvertently posting misinformation during elections.

Bing Search anticipated instances of information manipulation with possible actor intent to manipulate search algorithms and lead users to data voids and low-authority content related to elections. As part of its regular information integrity operations, Bing detected information manipulation themes related to the 2024 Romanian Presidential Election, which have been ingested to inform defensive search interventions.

Mitigations in place during the electoral period:

LinkedIn's Professional Community Policies expressly prohibit false and misleading content, including [misinformation and disinformation](#), and its in-house Editorial team provides members with trustworthy content regarding global events, including European Elections. LinkedIn had approximately 1,443 content moderators globally (for 24/7 coverage, with 180 content moderators located in the EU as at 31 December 2024). These reviewers use policies and guidance developed by a dedicated content policy team and experienced lawyers, and work with external fact checkers as needed. When LinkedIn sees content or behaviour that violates its Professional Community Policies, it takes action, including the removal of content or the restriction of an account for repeated abusive behaviour.

Political ads are banned on LinkedIn, which includes prohibitions on ads that exploit a sensitive political issue, including European Elections. LinkedIn also does not provide a mechanism for content creators to monetise the content they post on LinkedIn.

LinkedIn continues to mature its crisis response processes. Including 1) quickly coordinating with industry peers regarding the exchange of threat indicators; 2) engaging with external stakeholders regarding trends and TTPs; 3) continuously providing updated policy guidance to internal teams to assist with the removal of misinformation; and 4) continuing to proactively provide localised trustworthy information to our members.

LinkedIn has continued to mature its crisis response playbook by continually monitoring crisis situations globally, expanding internal teams that work on crisis response, and maturing our processes to respond more efficiently and effectively to crisis situations. LinkedIn will continue to follow its processes related to the removal of misinformation, and continually increase investments in resource allocation and process improvements where necessary to respond to the demands of the crisis.

LinkedIn also implemented a specialized intake and operations process under the Elections Working Group Rapid Response System for the Romanian Presidential elections.

Bing Search takes a multifaceted approach to protecting election integrity and regularly updates its processes, policies, and practices to adapt to evolving risks, trends, and technological innovations. This approach includes: (1) defensive search interventions; (2) regular direction of users to high authority, high quality sources as part of the search algorithm; (3) removal of auto suggest and related search terms considered likely to lead users to low authority content; (4) partnerships with independent organisations for threat intelligence on information manipulation, civic integrity and nation state affiliated actors to inform potential algorithmic interventions and contribute to broader research community; (5) special information panels and answers to direct users to high authority sources concerning elections and voting; (6) internal working groups dedicated to addressing company-wide election initiatives; (7) establishing special election-focused product feature teams; (8) conducting internal research on content provenance and elections; (9) evaluating and undertaking red-team testing for generative AI features with respect to elections and political content; (10) ensuring Responsible AI reviews for all AI features; (11) undertaking comprehensive risk assessments related to elections and electoral processes; (12) developing and continuing to improve targeted monitoring both for web search and Bing generative AI experiences; (13) restricting generative AI responses for certain types of election-related content; (14) leveraging blocklists and classifiers in generative AI experiences to restrict generation of images or certain types of content concerning political candidates and certain election-related topics; (15) integrating information on political parties, candidates, and elections from local election authorities (including in the EU) or high authority third party sources to inform defensive interventions and election-related product mitigations; and (16) regularly evaluating whether additional measures, metrics, or mitigations should be implemented. These measures are integrated into Bing Search and Bing generative AI experiences, along with the additional safeguards discussed at QRE 14.1.1 and QRE 14.1.2 and other measures discussed throughout this report.

Bing also participated in the Election Rapid Response System and roundtable discussion in November 2024 with EU member state authorities and the European Commission to discuss election-related learnings and general election response. Bing also undertakes internal post-election reviews, as appropriate, to evaluate product and mitigation performance, reflect on challenges and learnings, and identify potential areas for improvement. These reviews occur both in product review settings and in broader cross-functional teams dedicated to elections at Microsoft.

Bing also maintains an incident response process for cross-functional teams to prioritize high-risk incidents and track the investigation, fixes, and post-incident analysis. Internal escalation processes are set up to ensure urgent cases— including sensitive issues related to elections or election-related content -- are addressed expediently with high priority. Bing also implemented a specialized intake and operations process under the Elections Working Group Rapid Response System and coordinates with Democracy Forward Election Hubs on incidents.

Throughout the reporting period and in line with your commitments under the Tech Accord Microsoft and LinkedIn continued to take vital steps forward against AI deepfakes, which make it more difficult for malicious actors to use legitimate tools to create deepfakes targeting candidates, campaigns and election authorities. This work focused on content generation tools, strengthening the safety architecture in AI services by assessing risks and strengthening controls to help prevent abuse. This includes aspects such as ongoing red team analysis, preemptive classifiers, the blocking of abusive prompts, automated testing, and rapid bans of users who generate deceptive AI targeting elections.

We combined this work with the launch of an expanded Digital Safety Unit. This will extend the work of our existing digital safety team, which has long addressed abusive online content and conduct that impacts children or that promotes extremist violence, among other categories. This team has special ability in responding on a 24/7 basis to weaponized content from mass shootings that we act immediately to remove from our services. The accord's commitments oblige Microsoft and the tech sector to continue to

engage with a diverse set of global civil society organizations, academics, and other subject matter experts. These groups and individuals play an indispensable role in the promotion and protection of the world's democracies.

See more at [Microsoft announces new steps to help protect elections - Microsoft On the Issues](#) and [Meeting the moment: combating AI deepfakes in elections through today's new tech accord - Microsoft On the Issues](#).

In advance of the EU elections this summer we kicked off a global effort to engage campaigns and elections authorities to deepen understanding of the possible risks of deceptive AI in elections and empower those campaigns and election officials to speak directly to their voters about these risks steps they can take to build resilience and increase confidence in the election. This year we have conducted almost 200 training sessions for political stakeholders in 25 countries, reaching over 4300 participants. This includes almost fifty separate training events with nearly 500 participants...

As part of our commitments related to public awareness and engagement, Microsoft ran a campaign titled [Check. Recheck. Vote.](#) containing a series of public messages and stood up an AI and Elections [website](#) focused on engaging voters about the risks of deceptive AI and where to find authoritative election information. This campaign ran across the EU, UK, and the US in the lead up to major elections. Globally, the campaign reached hundreds of millions of people, with millions interacting with the content, connecting them with official election information.

In addition, Microsoft is harnessing the data science and technical capabilities of our AI for Good Lab and MTAC teams to better assess whether abusive content—including that created and disseminated by foreign actors—is synthetic or not. Microsoft AI for Good lab has been developing detection models (image, video) to assess whether media was generated or manipulated by AI. The model is trained on approximately 200,000 examples of AI and real content. AI for Good continues to invest in creating sample dataset representing the latest generative AI technology. When appropriate, we call on the expertise of Microsoft's Digital Crimes Unit to invest in and operationalize the early detection of AI-powered criminal activity and respond appropriately, through the filing of affirmative civil actions to disrupt and deter that activity and through threat intelligence programs and data sharing with customers and government.

We are also empowering candidates, campaigns and election authorities to help us detect and respond to deceptive AI targeting elections. We launched the Microsoft-2024 Elections site where candidates in a national or federal election can directly report deceptive AI election content on Microsoft consumer services. This reporting tool allows for 24/7 reporting by impacted election entities who have been targeted by deceptive AI found on Microsoft platforms.

[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].

Policies and Terms and Conditions

Outline any changes to your policies

Policy	Changes (such as newly introduced policies, edits, adaptation in scope or implementation)	Rationale
Bing Search		
Authoritative Information sources	Bing aims provide the high quality, authoritative content relevant to users' search terms. Our goal is to always provide fair, balanced, and comprehensive content. When there are multiple credible perspectives, we try to display them in informative ways. When there is no authoritative source, our goal is to avoid promoting bias or potentially misleading information. See more in How Bing delivers search results - Microsoft Support	
Microsoft		
Deepfakes and Elections	<p>Last year, Microsoft launched a new web page – Microsoft-2024 Elections – where political candidates can report alleged deepfakes of themselves to Microsoft. To date, we have not received an actionable report of deceptive AI targeting elections on Microsoft platforms.</p> <p>Microsoft's Office of Responsible AI has also established policies concerning election-related content and works with teams, including Bing and Bing Image Creator, on implementation.</p>	See more at Meeting the moment: combating AI deepfakes in elections through new tech accord
Content Integrity tools	During the reporting period, Microsoft continued piloting Content Integrity Tools, which allowed users to add content credentials to their own authentic content. Designed as a pilot program primarily to support the 2024 election cycle and gather feedback about Content Credentials-enabled tools, during the reporting period of this report, the tools were available to political campaigns in the EU, as well as to elections authorities and select news media organizations in the EU and globally. These tools included a partnership and collaboration with fellow Tech Accord signatory, TruePic. Announced in April 2024, this collaboration leveraged	These watermarking credentials empower an individual or organization to assert that an image or video came from them while protecting against tampering by showing if content was altered after its credentials were created. See more at Expanding our Content Integrity tools to support global elections - Microsoft On the Issues

	TruePic's mobile camera SDK enabling campaign, election, and media participants to capture authentic images, videos and audio directly from a vetted and secure device. Called the "Content Integrity Capture App" (an app that makes it easy to directly capture images with C2PA enabled signing) launched for both Android and Apple and can be used by participants in the Content Integrity Tools pilot program.	
Campaign Success Teams	Microsoft helps political campaigns navigate cybersecurity challenges and the new world of AI by deploying a newly formed "Campaign Success Team" within Microsoft Philanthropies' Tech for Social Impact organization. This team advises and supports campaigns as they navigate the world of AI, combat the spread of cyber influence campaigns, and protect the authenticity of their own content and images.	See more at Microsoft announces new steps to help protect elections - Microsoft On the Issues
AI Elections Trainings	In advance of the elections across the EU, we kicked off a global effort to engage campaigns and elections authorities to deepen understanding of the possible risks of deceptive AI in elections and empower those campaigns and election officials to speak directly to their voters about these risks steps they can take to build resilience and increase confidence in the election. In 2024, we have conducted almost 200 training sessions for political stakeholders in 25 countries, reaching over 4300 participants. This includes almost fifty separate training events with nearly 500 participants.	
Communications Hub	Microsoft created and provides access to a new "Election Communications Hub" to support democratic governments around the world as they build secure and resilient election processes.	See more at Microsoft announces new steps to help protect elections - Microsoft On the Issues

Foreign Malign Influence Updates	<p>Microsoft publishes regular reports on foreign malign influence researched and reported by the company's MTAC team. The first report was released in November 2023.</p> <p>Microsoft also published MTAC analysis on how Russian US election interference targets support for Ukraine in April 2024. This election report provides an update on what Microsoft has observed from Russia, Iran, and China and malicious use of AI since our November 2023 report.</p>	<p>See more at Microsoft announces new steps to help protect elections - Microsoft On the Issues</p> <p>See more at Meeting the moment: combating AI deepfakes in elections through new tech accord</p> <p>See more at Russian US election interference targets support for Ukraine after slow start - Microsoft On the Issues</p>
LinkedIn		
False or misleading content	<p>LinkedIn continually updates its policies as appropriate during any major global event, including European elections.</p>	<p>Misinformation, disinformation campaigns, coordinated manipulative behaviours, malicious use of advertising products, and the involvement of foreign state actors, are all harms that existed prior to the recently-concluded European elections, and therefore LinkedIn already had policies in place to address these harms.</p>
Scrutiny of Ads Placements		
<p>Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.</p>		
LinkedIn		
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>Political ads are banned on LinkedIn, which includes prohibitions on ads that exploit a sensitive political issue, including European Elections.</p> <p>LinkedIn does not pay its members for creating content, other than in rare instances where we individually select and manage a small group of content creators to create professionally-relevant content.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>n/a</p>	

Microsoft Advertising	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention As described in Section 3 of the report, Microsoft Advertising does not support political advertising.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available During the relevant reporting period, Microsoft Advertising blocked 19 phrases, which I prevented future keyword or ad submissions for the Romanian election candidates and parties.
Political Advertising	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention Political ads are banned on LinkedIn, which includes prohibitions on ads that exploit a sensitive political issue, including European Elections.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available n/a
Microsoft Advertising	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention Not applicable. As described in Section 3 of the report, Microsoft Advertising does not support political advertising.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available n/a
Integrity of Services	

Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention
	<p>LinkedIn also maintains a robust automated and manual ad-review process to prevent ads related to European elections from running on our platform.</p> <p>LinkedIn regularly meets with and exchanges information with industry peers to identify and share granular information related to manipulative behaviours, coordinated influence operations, and TTPs. All such content that violates LinkedIn's Professional Community Policies is removed.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>LinkedIn does not track misinformation content removal by subject matter, and a comprehensive listing of its misinformation content takedowns is provided in this disclosure and in its Transparency Report. See also SLI 18.2.1.</p> <p>Impact metrics for malicious advertising removals are available in SLI 2.1.1 and 2.3.1, whereas metrics related to manipulative behaviors and TTPs are available in SLI 12.1.1 and 14.2.1.</p>
Bing Search	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>Bing Search takes a multifaceted approach to protecting election integrity and regularly updates its processes, policies, and practices to adapt to evolving risks, trends, and technological innovations. This approach includes: (1) defensive search interventions; (2) regular direction of users to high authority, high quality sources; (3) removal of auto suggest and related search terms considered likely to lead users to low authority content; (4) partnerships with independent fact checkers, research and nonprofit organisations to maintain threat intelligence and inform potential algorithmic interventions and contribute to broader research community; (5) special information panels and answers to direct users to high authority sources concerning elections and voting; (6) internal working groups dedicated to addressing company-wide election initiatives; (7) establishing special election-focused product feature teams; (8) conducting internal research on content provenance and elections; (9) evaluating and undertaking red-team testing for generative AI features with respect to elections and political content; (10) ensuring Responsible AI reviews for all AI features; (11) undertaking comprehensive risk assessments related to elections and electoral processes; (12) developing and continuing to improve targeted monitoring both for web search and Bing Generative AI experiences; (13) restricting generative AI responses for certain types of election-related content; (14) leveraging blocklists and classifiers in Bing generative AI experiences to restrict generation of images or certain types of content concerning political candidates and certain election-related topics; (15) integrating information on political parties, candidates, and elections from local election authorities or high authority third party sources to inform defensive interventions and election-related product mitigations; (16) working</p>

	<p>with reputable third parties to test election-related responses in Bing generative AI experiences r; and (17) regularly evaluating whether additional measures, metrics, or mitigations should be implemented. These measures are integrated into Bing Search and Bing generative AI experiences, along with the additional safeguards discussed at QRE 14.1.1 and QRE 14.1.2 and other measures discussed throughout this report.</p> <p>Bing participated in post-election roundtable sessions to share learnings with the European Commission and Romania's local DSC in November 2024.. Bing also undertakes internal post-election reviews, as appropriate, to evaluate product and mitigation performance, reflect on challenges and learnings, and identify potential areas for improvement. These reviews occur both in product review settings and in broader cross-functional teams dedicated to elections at Microsoft.</p> <p>Given the rapid response required to respond to urgent election issues, Bing maintained an incident response process for cross-functional teams to prioritize high-risk incidents and track the investigation, fixes, and post-incident analysis. Internal escalation processes are set up to ensure urgent cases-- including sensitive issues related to elections or election-related content -- are addressed expediently with high priority. Bing also implemented a specialized intake and operations process under the Elections Working Group Rapid Response System and coordinates with broader Microsoft Election Hubs on incidents.</p> <p>Through Microsoft's Democracy Forward team, Bing has also integrated information on political parties, candidates, and elections from local election authorities or high authority third party sources to inform defensive interventions and election-related product mitigations.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <ul style="list-style-type: none"> • Bing identified a numerous information manipulation themes related to the Romanian Presidential election, which have informed defensive search interventions and fanouts to related search terms.
Empowering Users	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	
Specific Action applied (with reference to the Code's relevant	<p>Description of intervention</p> <p>LinkedIn has an internal team of global news editors that provides trustworthy and authoritative content to its member-base at all times. During important events in European elections, this team provides manually curated and localised storylines.</p>

Commitment and Measure)	Indication of impact (at beginning of action: expected impact) including relevant metrics when available
Bing Search	
Partnerships with Election Authorities and Trusted Partners (with reference to the Code's relevant Commitment and Measure)	Description of intervention Bing Search empowers voters with authoritative election information on Bing. Bing does this in partnership with organizations that provide information on authoritative sources, ensuring that queries about election administration will surface reputable sites.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available
Empowering the Research Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Bing Search	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	Description of intervention None for Bing
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available N/A
LinkedIn	
Specific Action applied (with reference to the Code's relevant	Description of intervention None for LinkedIn

Commitment and Measure)	
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>None for LinkedIn</p>
Empowering the Fact-Checking Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
LinkedIn	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>LinkedIn works with globally-recognised factcheckers to receive their independent judgment regarding user-generated content. Content that violates LinkedIn's policy on false and misleading content is removed.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>LinkedIn does not separately track election related content sent to external fact checkers. Further detail regarding content sent to fact checkers is available at SLI 21.1.1, 30.1.1, and 31.1.1.</p>
Bing Search	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	<p>Description of intervention</p> <p>Articles from news and fact checking organizations may also appear as part of specialized Bing Answers. In addition, news and fact-check articles can appear in Bing News carousels, which are often presented at the top of search results pages, depending on the nature of user query. Microsoft maintains agreements with news publishers to surface high authority content, including articles from well-regarded fact checking organizations and journalist-driven fact-checks, high in relevant search results.</p> <p>Bing utilizes threat intelligence to inform the Bing algorithm and defensive search measures for Bing search and Bing generative AI experiences. Bing works with trusted third-party partners for leads of potential threats (including in EEA member state languages) to inform defensive search strategies. Bing also utilises the ClaimReview open protocol to ingest fact checks into search results. To improve coverage during the Reporting Period Bing also leveraged fact check intelligence from European Digital Media Observatory.</p>

	Bing increased the coverage of EEA member state languages, informing interventions across monitored themes and sources.
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>n/a</p>
Microsoft	
<p>Specific Action applied (with reference to the Code’s relevant Commitment and Measure)</p>	<p>Description of intervention</p> <p>In December 2023, the Institute for Nonprofit News teamed up with DeleteMe, funded by Microsoft’s Democracy Forward Initiative, to help decrease the amount of personal information about journalists that can be discovered online. The collaboration protects local journalists from threats during a critical election year and ensures they can provide high-quality information to local communities. The Microsoft Journalism Hub is an ongoing resource center built to connect the journalism community more seamlessly with tools, technology, services, and partner programs designed to support their unique business needs. These resources are distributed across Microsoft’s three journalism initiative commitments: rebuilding capacity in local news ecosystems; restoring trust in news; and reducing legal and cyber risks for journalists.</p> <p>Microsoft has partnered with Nota to allow journalists to access helpful AI tools for tasks such as improving SEO, creating videos of published stories, and writing headlines. Nota’s assistive AI tools build time-saving production infrastructure for digital publishing—creating an accessible engagement economy, offering instant content conversion and content amplification, multiplying video content revenue and doing away with repetitive tasks that have long required journalists to act as generalists in multiple fields.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>n/a</p>