



Code of Practice on Disinformation – Report of TikTok for the period 1 July 2023 - 31 December 2023



Table of Contents

II. Scrutiny of Ad Placements.....	15
Commitment 1.....	16
Commitment 2.....	29
Commitment 3.....	38
III. Political Advertising.....	41
Commitment 4.....	42
Commitment 5.....	43
Commitment 6.....	44
Commitment 8.....	48
Commitment 9.....	49
Commitment 10.....	50
Commitment 11.....	51
Commitment 12.....	52
Commitment 13.....	53
IV. Integrity of Services.....	55
Commitment 14.....	56
Commitment 15.....	87
Commitment 16.....	89
V. Empowering Users.....	92
Commitment 17.....	93
Commitment 18.....	136
Commitment 19.....	152
Commitment 20.....	158
Commitment 21.....	159
Commitment 22.....	171
Commitment 23.....	179
Commitment 24.....	185
Commitment 25.....	192
VI. Empowering the research community.....	194
Commitment 26.....	195
Commitment 27.....	201
Commitment 28.....	203
Commitment 29.....	207
VII. Empowering the fact-checking community.....	210
Commitment 30.....	211
Commitment 31.....	219
Commitment 32.....	228
Commitment 33.....	230
VIII. Transparency Centre.....	232



Commitment 34.....	233
Commitment 35.....	234
Commitment 36.....	235
IX. Permanent Task-Force.....	237
Commitment 37.....	238
X. Monitoring of Code.....	240
Commitment 38.....	241
Commitment 39.....	242
Commitment 40.....	243
Commitment 41.....	244
Commitment 42.....	245
Commitment 43.....	246
Commitment 44.....	246
War of aggression by Russia on Ukraine.....	249
Israel - Hamas Conflict.....	262
European Elections.....	275



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



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



17	Measure 17.1	<input checked="" type="checkbox"/>
	Measure 17.2	<input checked="" type="checkbox"/>
	Measure 17.3	<input checked="" type="checkbox"/>
18	Measure 18.1	<input checked="" type="checkbox"/>
	Measure 18.2	<input checked="" type="checkbox"/>
	Measure 18.3	<input checked="" type="checkbox"/>
19	Measure 19.1	<input checked="" type="checkbox"/>
	Measure 19.2	<input checked="" type="checkbox"/>
20	Measure 20.1	<input type="checkbox"/>
	Measure 20.2	<input type="checkbox"/>
21	Measure 21.1	<input checked="" type="checkbox"/>
	Measure 21.2	<input checked="" type="checkbox"/>
	Measure 21.3	<input checked="" type="checkbox"/>
22	Measure 22.1	<input type="checkbox"/>
	Measure 22.2	<input type="checkbox"/>
	Measure 22.3	<input type="checkbox"/>
	Measure 22.4	<input type="checkbox"/>
	Measure 22.5	<input type="checkbox"/>
	Measure 22.6	<input type="checkbox"/>
	Measure 22.7	<input checked="" type="checkbox"/>
23	Measure 23.1	<input checked="" type="checkbox"/>
	Measure 23.2	<input checked="" type="checkbox"/>
24	Measure 24.1	<input checked="" type="checkbox"/>
25	Measure 25.1	<input type="checkbox"/>
	Measure 25.2	<input type="checkbox"/>
VI. Empowering the research community		
26	Measure 26.1	<input checked="" type="checkbox"/>



	Measure 26.2	<input checked="" type="checkbox"/>
	Measure 26.3	<input checked="" type="checkbox"/>
27	Measure 27.1	<input checked="" type="checkbox"/>
	Measure 27.2	<input checked="" type="checkbox"/>
	Measure 27.3	<input checked="" type="checkbox"/>
	Measure 27.4	<input checked="" type="checkbox"/>
28	Measure 28.1	<input checked="" type="checkbox"/>
	Measure 28.2	<input checked="" type="checkbox"/>
	Measure 28.3	<input checked="" type="checkbox"/>
	Measure 28.4	<input checked="" type="checkbox"/>
29	Measure 29.1	<input type="checkbox"/>
	Measure 29.2	<input type="checkbox"/>
	Measure 29.3	<input type="checkbox"/>
VII. Empowering the fact-checking community		
30	Measure 30.1	<input checked="" type="checkbox"/>
	Measure 30.2	<input checked="" type="checkbox"/>
	Measure 30.3	<input checked="" type="checkbox"/>
	Measure 30.4	<input checked="" type="checkbox"/>
31	Measure 31.1	<input checked="" type="checkbox"/>
	Measure 31.2	<input checked="" type="checkbox"/>
	Measure 31.3	<input checked="" type="checkbox"/>
	Measure 31.4	<input checked="" type="checkbox"/>
32	Measure 32.1	<input checked="" type="checkbox"/>
	Measure 32.2	<input checked="" type="checkbox"/>
	Measure 32.3	<input checked="" type="checkbox"/>
33	Measure 33.1	<input type="checkbox"/>
VIII. Transparency centre		



34	Measure 34.1	<input checked="" type="checkbox"/>
	Measure 34.2	<input checked="" type="checkbox"/>
	Measure 34.3	<input checked="" type="checkbox"/>
	Measure 34.4	<input checked="" type="checkbox"/>
	Measure 34.5	<input checked="" type="checkbox"/>
35	Measure 35.1	<input checked="" type="checkbox"/>
	Measure 35.2	<input checked="" type="checkbox"/>
	Measure 35.3	<input checked="" type="checkbox"/>
	Measure 35.4	<input checked="" type="checkbox"/>
	Measure 35.5	<input checked="" type="checkbox"/>
	Measure 35.6	<input checked="" type="checkbox"/>
36	Measure 36.1	<input checked="" type="checkbox"/>
	Measure 36.2	<input checked="" type="checkbox"/>
	Measure 36.3	<input checked="" type="checkbox"/>
IX. Permanent Task-Force		
37	Measure 37.1	<input checked="" type="checkbox"/>
	Measure 37.2	<input checked="" type="checkbox"/>
	Measure 37.3	<input checked="" type="checkbox"/>
	Measure 37.4	<input checked="" type="checkbox"/>
	Measure 37.5	<input checked="" type="checkbox"/>
	Measure 37.6	<input checked="" type="checkbox"/>
X. Monitoring of the Code		
38	-	<input checked="" type="checkbox"/>
39	-	<input checked="" type="checkbox"/>
40	Measure 40.1	<input checked="" type="checkbox"/>
	Measure 40.2	<input checked="" type="checkbox"/>
	Measure 40.3	<input checked="" type="checkbox"/>



	Measure 40.4	☒
	Measure 40.5	☒
	Measure 40.6	☒
41	Measure 41.1	☒
	Measure 41.2	☒
	Measure 41.3	☒
42	-	☒
43	-	☒
44	-	☒



Executive summary

About TikTok

TikTok's mission is to inspire creativity and bring joy. Ensuring the safety, privacy, and security of our community is critical to achieving that goal.

We treat disinformation with the utmost seriousness and are committed to preventing its spread, while elevating authoritative information and investing in media literacy to help build resilience among our community against misinformation. At TikTok, we place considerable emphasis on proactive content moderation and are proud that the vast majority of violative content is identified and removed proactively before it receives any views or is reported to us. Violations of our harmful misinformation policies make up around 1 % of overall video removals within the EU/European Economic Area (EEA). We are also committed to continuing to keep pace with evolving issues that affect our users.

As part of the Digital Services Act (DSA) compliance programme, under which the Code of the Practice of Disinformation (the Code) will find a new legislative home, we have [implemented](#) a range of measures designed to keep our users safe across a number of key areas, including disinformation. Further information on TikTok's approach to DSA compliance can be found on our [European Online Safety Hub](#). Our work under the Code continues to reflect our strong commitment to combatting disinformation on our platform and to providing transparency to our wider community about the measures we take.

Our third report under the Code - 1 July to 31 December 2023

Since 2020, TikTok has been committed to, and heavily involved in, the Code process. We continue to meaningfully engage in the Code's Taskforce and all of its working groups and subgroups. TikTok is co-chair of the working group on Elections and has joined the newly created Generative AI working group.

The positive reception TikTok received to its baseline report underlines the significant resources and time we have committed across many teams to the Code. We set a high bar in our first report as we provided detailed descriptions of the measures we take and disclosed robust, granular data in support of those measures.

In our second and third reports, we continued to build on our existing measures and increased the number of data points disclosed enabling us to further enhance transparency for our community.

In this third report, we are pleased to report on the launch of new tools, such as our AI labelling tool which allows users to self-disclose AI-generated content when posting, as well as more granular harmful misinformation ad policies that we've begun to implement. We also disclose new metrics, including on the use of our Research and Commercial Content APIs that bring transparency on both organic and paid and commercial content that is available on our platform.

We are proud of our continued efforts to protect our community against disinformation and to empower them with the tools they need to be resilient in the face of new misinformation trends.

Our policies

Our Integrity and Authenticity policies aim to promote a trustworthy, authentic experience for our users. Our policies focus on harmful misinformation (rather than making a distinction between disinformation and



misinformation) and deceptive behaviours.¹ We do not allow inaccurate, misleading, or false content that may cause significant harm to individuals or society, regardless of intent. These policies can be applied to a wide range of content, and that's by design; this content is constantly changing, often based on what's happening in the world. We also tackle deceptive behaviour by removing accounts that seek to mislead people or attempt to use TikTok to deceptively sway public opinion.

In the spirit of continuous improvement, we are always reviewing and developing our policies.

Enforcing our policies

At TikTok, over 40,000 safety professionals work every day to keep people on TikTok safe. To do this effectively at scale, we continue to strengthen our automated review process and invest in training for our Trust and Safety team. We have provided more transparency to our community on [how we moderate](#) and what [moderation actions we take](#). This includes more detail about what content we make ineligible for the For You feed. We disclose in this report the underlying metrics.

While we rely on automated moderation when our systems have a high degree of confidence that content is violative, disinformation differs from other content issues and context and fact-checking are critical. While we use machine learning models to help detect potential misinformation, our approach entails having our trained misinformation moderation team assess, confirm, and remove harmful misinformation violations. Our moderators have access to [independent fact-checking partners](#) and our database of previously fact-checked claims to help assess the accuracy of content.

By expanding our fact-checking programme to two new EU countries (Croatia and Portugal) over the past six months, and together with expanding our moderation teams trained on misinformation and strengthening our machine learning models, our numbers show our increased ability to remove more complex harmful misinformation.

Transparency and Scrutiny of Advertising

Ads must comply with and are reviewed against our [ad policies](#) before being allowed on our platform. These policies specifically prohibit misleading, inauthentic and deceptive behaviours. We launched four more granular harmful misinformation ad policies as part of our continuous improvement, covering medical misinformation, dangerous misinformation, manipulated media and dangerous conspiracy theories.

We continue to engage with external stakeholders in order to increase the effectiveness of our scrutiny of ad placements. As a Global Alliance for Responsible Media (GARM) member, we also remain committed to upholding the GARM Framework and, as part of that, removing harmful misinformation from monetisation.

Like all users of our platform, participants in content monetisation programs must adhere to our [Community Guidelines](#), including our Integrity and Authenticity policies. Those policies make clear that we do not allow activities that may undermine the integrity of our platform or the authenticity of our users. They also make clear that we remove content or accounts, including those of creators, which contain misleading information that causes significant harm or deceptive behaviours. In certain scenarios, we may remove a creator's access to a creator monetisation feature.

¹ At TikTok, we take action to moderate or remove content containing harmful misinformation, irrespective of intent (i.e. whether or not the content in question amounts to disinformation), in accordance with our Community Guidelines. For the purposes of alignment with the Code, throughout this report, we use "misinformation" and "disinformation" interchangeably.



Prohibiting Paid Political Ads

TikTok is first and foremost an entertainment platform, and we're proud to be a place that brings people together over creative and entertaining content. We do not allow anyone to place [political ads](#), nor do we allow politicians and political party accounts to place ads. We also prevent [governments, politicians and political party accounts](#) ("GPPAs") from accessing our monetisation features and campaign fundraising.

Sharing political beliefs and engaging in political conversation is allowed as organic content, but our policies prohibit users from paying to advertise or promote this content. We also allow some cause based advertising and public services advertising from government agencies, non-profits and other entities provided they are not driven by partisan political motives.

We are pleased that the EU Regulation on Transparency of Political Advertising was recently adopted and are carefully considering the potential impact on our policies.

By prohibiting political ads, campaign fundraising and limiting access to certain monetisation features, we're aiming to strike a balance between enabling people to discuss the issues that are relevant to their lives while also protecting the creative, entertaining platform that our community wants.

Ensuring the Integrity of Services

Our Integrity and Authenticity policies ([I&A policies](#)) robustly prohibit deceptive behaviours and we use a range of tactics, techniques and procedures to enforce those policies.

Our synthetic media policy addresses the use of content created or modified by AI technology on our platform. While we welcome the creativity that new AI may unlock, users must proactively disclose when their content is AI-generated or manipulated but shows realistic scenes. In order to facilitate compliance with this requirement, we've launched our [AI-generated label](#) for creators to disclose content that is completely AI-generated or significantly edited by AI. Similarly, in an effort to further help our users identify AI-generated content, any TikTok effect that uses AI will now explicitly include an "AI" mention in the effect name and the corresponding effect label.

We continue to fight against covert influence operations (CIO) and we do not allow attempts to sway public opinion while misleading our platform's systems or community about the identity, origin, operating location, popularity, or purpose of the account. CIOs continue to evolve in response to our detection and networks may attempt to re-establish a presence on our platform. This is why we continue to iteratively research and evaluate complex deceptive behaviours and develop appropriate product and policy solutions. We continue to provide information about the CIO networks we identify and remove in this report and within our transparency reports [here](#). In the coming months, we will introduce dedicated CIOs reports to further increase transparency, accountability, and cross-industry sharing.

Empowering Users

If a user encounters content that violates our Community Guidelines or contains suspected illegal content, our in-app reporting tools are accessible and simple to use.

Together with systematically removing content from our platform that violates our policies, we have dedicated significant resources to increasing the number of in-app measures that show users additional context on certain content, redirect them to authoritative information and encourage them to report any potential misinformation on the topic. We keep under review what topics to develop interventions for, including on climate change, the War in Ukraine and the Israel / Hamas conflict. We make these tools available in 23 official languages.



We continue to be involved in a variety of on and off-platform media literacy campaigns in close collaboration with our fact-checking partners, particularly in relation to local elections. We rolled out localised election integrity campaigns in advance of the elections which took place in the Netherlands, Poland, Slovakia and Spain. In total, in 2023, we launched media literacy campaigns in 18 European countries, generating over 220m impressions and reaching approx. 50m people on TikTok. This work will continue this year, with nine additional campaigns scheduled to go live in 2024 as well as localised media literacy activations in all 27 EU Member States ahead of the EU Elections in June 2024.

As we believe collaboration helps strengthen our efforts to protect against harm and misuse on our platform, as part of our Election Speaker Series, we invite external experts, particularly from the fact-checking community, to share their insights and market expertise with our internal team in order to inform our approach to elections.

We are also pleased to report that we have expanded the availability of our state-controlled media label to Sub-Saharan Africa, further increasing transparency for EU users.

Empowering Researchers

We recognise the important role of researchers in helping to identify disinformation trends and practices.

We have been publishing our [Community Guidelines Enforcement Reports](#) since 2020 in order to bring transparency around how we operate and protect our platform. Since we expanded our [Research API](#) (which provides researchers with access to public data on content and accounts from our platform) to Europe and rolled-out a number of [improvements](#), we've approved 49 applications to access and use this API from EEA researchers. We have also received more than 50 applications in the region to access our [Commercial Content API](#) that brings transparency to paid advertising and other content that's commercial in nature on TikTok.

Empowering the Fact-Checking Community

TikTok recognises the important contribution of fact-checkers to the fight against disinformation.

Our fact-checking programme incorporates fact-checker input into our broader content moderation efforts. This means that this feedback is relayed to TikTok's moderation teams so that they can ensure it is factored into their moderation work. This approach effectively produces a force multiplier to the underlying fact-checking output, ensuring that the disinformation content or trend is more comprehensively and broadly addressed. Our fact-checking repository, that we have continued to expand, ensures that our teams and systems leverage the full scope of insights our fact-checking partners submit to TikTok.

We have continued to progress the scale-up of our fact-checking program across Europe and we have launched fact-checking programs in Croatia and Portugal and onboarded two new fact-checking partners, meaning that we now have coverage in 18 official EU languages and the spoken language of 24 EEA countries.

Our efforts to scale-up our fact-checking coverage will allow us to cover at least one official language of each of the European Member States ahead of the 2024 EU Parliamentary Elections.

Looking forward

TikTok is proud to be part of this cross-industry initiative in tackling disinformation. We recognise that collaboration across the ecosystem is critical to efforts to eradicate the conditions for harmful disinformation and deceptive behaviour to flourish on platforms. TikTok looks forward to continued collaboration with the industry and other partners through the Code's Taskforce and all of its working groups and subgroups.



We are committed to continuing to develop and enhance our policies and tools ahead of the next Code report.



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

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].

- Launched four new ad policies in the EEA, which are aligned with our existing policies but provide increased granularity. The new policies cover:
 - Medical Misinformation
 - Dangerous Misinformation
 - Manipulated Media
 - Dangerous Conspiracy Theories
- Expanded the operational coverage in the EEA of our in-house pre-campaign brand safety tool, the TikTok Inventory Filter.
- Increased the implementation of our third party post-campaign brand safety solutions provided by Integral Ad Science (**IAS**) and Zefr within the EU.
- Increased transparency around harmful misinformation and ads and have disclosed a number of additional metrics for this Chapter of the report.



	<ul style="list-style-type: none"> Continued to regularly participate in the working group on Ad Scrutiny.
<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]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> Globalising and improving the implementation and enforcement of our four new harmful misinformation ad policies. Continuing to explore whether we should develop further policies targeted at specific types of harmful misinformation to increase the granularity of our ad policies. Continuing to review our third party pre-campaign and post-campaign brand safety solutions and working to expand our operational coverage where there is a demand. Continuing our engagement with relevant players such as GARM, IAB Sweden and IAB Ireland.
<p>Measure 1.1</p>	
<p>QRE 1.1.1</p>	<p>To help keep our platform welcoming and authentic for everyone, we take seriously ensuring it is free from harmful misinformation.</p> <p>(I) Our policies and approach</p> <p>Our Integrity and Authenticity (I&A) policies within our Community Guidelines (CGs) are the first line of defence in combating harmful misinformation and deceptive behaviours on our platform. All users are required to comply with our CGs, which set out the circumstances where we will remove, or otherwise limit the availability of, content.</p> <p>Paid ads are also subject to our ad policies and are reviewed against these policies before being allowed on our platform. Our ad policies specifically prohibit inaccurate, misleading, or false content that may cause significant harm to individuals or society, regardless of intent. They also prohibit other misleading, inauthentic and deceptive behaviours. Ads deemed in violation of these policies will not be permitted on our platform, and accounts deemed in severe or repeated violation may be suspended or banned.</p>



We are pleased to confirm that in order to improve our existing ad policies, we launched four new, more granular policies in the EEA in July. The new policies cover:

- Medical Misinformation
- Dangerous Misinformation
- Manipulated Media
- Dangerous Conspiracy Theories

We are now working on globalising the implementation of these policies.

We also have other, existing ad policies that focus on certain topics where the risk of disinformation may be higher. By way of example, our [Covid-19 ad policy](#) prohibits ads which present Covid-19 in a distasteful manner, for example manipulating consumers' fear or anxiety, or spreading harmful misinformation to push sales. As well as ensuring ads relating to Covid-19 do not spread harmful misinformation, we also promote authoritative sources of information. We have provided free ad credits to health authorities, governments, and non-profits to increase vaccine adoption, debunk vaccine myths and promote trustworthy Covid-19 resources.

We are continually reflecting on whether there are further focused areas for which we should develop new policies. Our [ad policies](#) require advertisers to meet a number of requirements regarding the landing page. For example, the landing page must be functioning and must contain complete and accurate information including about the advertiser. Ads risk not being approved if the product or service advertised on the landing page does not match that included in the ad.

In line with our approach of building a platform that brings people together, not divides them, we have long [prohibited political ads](#) and political [branded content](#). Specifically, we do [not allow paid ads](#) (nor landing pages) that promote or oppose a candidate, current leader, political party or group, or content that advocates a stance (for or against) on a local, state, or federal issue of public importance in order to influence a political decision or outcome. Similar rules apply in respect of branded content. We also do not allow [political actors to place ads](#)² and we have introduced restrictions at an account level. This means accounts belonging to politicians and political parties will automatically have their access to advertising features turned off. We make exceptions for governments in certain circumstances e.g., to promote public health.

We make various brand safety tools available to advertisers to assist in helping to ensure that their ads are not placed adjacent to content they do not consider to fit with their brand values. While any content that is violative of our CGs, including our I&A policies, is removed, the brand safety tools are designed to help advertisers to further protect their brand. For example, a family-oriented brand may not want to appear next to videos containing news-related content. As a GARM member, we believe in its mission and have adopted GARM's Brand Safety Floor and Suitability Framework (the **GARM Framework**).

(II) Verification in the context of ads

² See the 'Political and Issue Based Advertising' section



	<p>We provide verified badges on some accounts including certain advertisers. Verified badges help users make informed choices about the accounts they choose to follow. It's an easy way for notable figures to let users know they're seeing authentic content, and it helps to build trust among high-profile accounts and their followers. For individuals, non-profits, institutions, businesses, or official brand pages, this badge builds an important layer of clarity with the TikTok community. We consider a number of factors before granting a verified badge, such as whether the notable account is authentic, unique, and active.</p> <p>In the EU, we apply an internal label to accounts belonging to a government, politician, or political party. Once an account has been labelled in this manner, a number of policies will be applied that help prevent misuse of certain features e.g., access to advertising features and solicitation for campaign fundraising are not allowed.</p>		
<p>SLI 1.1.1 – Numbers by actions enforcing policies above (specify if at page and/or domain level)</p>	<p>Methodology of data measurement:</p> <p>We have set out the number of ads that have been removed from our platform for violation of our Covid-19 misinformation and political content policies, as well as our new, more granular policies on medical misinformation, dangerous misinformation, manipulated media and dangerous conspiracy theories.</p> <p>The majority of ads that violate our newly launched misinformation policies would have been removed under our existing policies. In cases where an ad is deemed violative of other policies and also for these additional misinformation policies, the removal is counted under the older policy. Therefore, the third column below shows only the number of ads removed where the sole reason was one of these four additional misinformation policies, and does not include ads already removed under our existing policies or where misinformation policies were not the driving factor for the removal.</p> <p>The data below suggests that our existing policies (such as political content and covid 19 misinformation policies, in addition to other policy areas such as our inaccurate, misleading, or false content policy) already cover the majority of harmful misinformation ads, due to their expansive coverage.</p> <p>Note that numbers have only been provided for monetised markets and are based on where the ads were displayed.</p>		
<p>Member States</p>	<p>Number of ad removals under the Covid-19 misinformation ad policy</p>	<p>Number of ad removals under the political content ad policy</p>	<p>Number of additional ad removals under the new misinformation ad policies</p>
<p>Austria</p>	<p>0</p>	<p>45</p>	<p>0</p>



Belgium	0	51	0
Bulgaria	N/A	N/A	N/A
Croatia	N/A	N/A	N/A
Cyprus	N/A	N/A	N/A
Czech Republic	0	18	0
Denmark	0	27	0
Estonia	N/A	N/A	N/A
Finland	0	16	0
France	0	140	0
Germany	1	272	1
Greece	0	0	0
Hungary	0	50	0
Ireland	0	33	0
Italy	0	94	0



Latvia	N/A	N/A	N/A
Lithuania	N/A	N/A	N/A
Luxembourg	0	0	0
Malta	N/A	N/A	N/A
Netherlands	0	62	7
Poland	1	163	0
Portugal	0	16	0
Romania	0	134	0
Slovakia	N/A	N/A	N/A
Slovenia	N/A	N/A	N/A
Spain	1	118	1
Sweden	0	33	0
Iceland	N/A	N/A	N/A
Liechtenstein	N/A	N/A	N/A
Norway	0	37	0



Total EU	3	1272	9
Total EEA	3	1309	9

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/bid³ or impression⁴) and applying an agreed-upon conversion factor provided by a third party designated by the Task-force of the Code (Ebiquity plc.).

<p>SLI 1.1.2 - Preventing the flow of legitimate advertising investment to sites or content that are designated as disinformation</p>	<p>The EU Code of Practice Permanent Task-force appointed Ebiquity Plc to serve in the capacity of ‘third-party estimator’, responsible for providing periodic Cost Per Mille (CPM) conversion factors for use by signatories to derive financial estimates solely in relation to this SLI. This SLI applies the conversion factor developed by Ebiquity to the impressions of ads that have been removed from our platform and aims to provide an estimate of the unrealised value of revenue related to the demonetisation of disinformation.</p> <p>The CPM data is provided on a specific EU market basis where available, and currently covers 26 of the 27 EU markets (excluding Luxembourg). Note that we have only provided numbers for monetised markets, based on where the ads were displayed.</p> <p>Ebiquity creates the CPM estimates based on aggregated and anonymized media investment data from their Media Data Vault, its proprietary database infrastructure used to service its clients. Ebiquity has developed three dedicated channel CPMs (Programmatic – Display, Programmatic - Online Video, and Paid Social) as well as a Blended CPM, which can be used for general application and is not identifiable to any specific client, agency, vendor, platform, or ad format.</p> <p>We have calculated the approximate financial value by using the "Blended CPM" value provided by Ebiquity. We note that this SLI provides an approximate financial value only, and does not reflect how TikTok monetises ad content in practice. It is therefore not an accurate representation of TikTok’s actual revenue.</p>
--	--

³ 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.

⁴ 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).



	TikTok was not involved in the development of the conversion factor and therefore cannot endorse it or the underlying methodology and data. We remain committed to increasing transparency in this chapter, including by participating in the working group to better understand the underlying methodology and ensure the conversion factor provides, as accurately as possible, an approximation of the financial value of actions taken to demonetise disinformation.				
Member States	Euro value of ads demonetised				
	Number of impressions for ads removed under the Covid-19 misinformation ad policy	Number of impressions for ads removed under the political content ad policy	Number of impressions for ads removed under the additional granular misinformation medical misinformation ad policies	Ebiquity Conversion	Euro Value of Ads Demonetised/1000 (accounting for Cost per thousand)
Austria	0	397,478	2,808	3.5	1401.001
Belgium	0	3,222,659	0	4	12890.636
Bulgaria	N/A	N/A	N/A	1.5	N/A
Croatia	N/A	N/A	N/A	1.5	N/A
Cyprus	N/A	N/A	N/A	2.5	N/A
Czech Republic	0	238,887	0	2.5	597.2175
Denmark	0	415,632	0	6	2493.792
Estonia	N/A	N/A	N/A	2.5	N/A



Finland	0	1,047,991	1,030	4.5	4720.5945
France	0	2,784,405	3,518	2.5	6969.8075
Germany	0	3,661,928	1,935	4	14655.452
Greece	0	0	0	1.5	0
Hungary	0	1,038,921	5,850	1.5	1567.1565
Ireland	0	391,170	0	2.5	977.925
Italy	0	3,619,351	5,931	1.5	5437.923
Latvia	N/A	N/A	N/A	3	N/A
Lithuania	N/A	N/A	N/A	1.5	N/A
Luxembourg	0	0	0	0	0
Malta	N/A	N/A	N/A	3	N/A
Netherlands	0	842,172	601	4	3371.092
Poland	0	4,958,443	206	1.5	7437.9735
Portugal	0	271,334	0	1.5	407.001



Romania	2,979	2,538,958	0	2	5083.874
Slovakia	N/A	N/A	N/A	2.5	N/A
Slovenia	N/A	N/A	N/A	1.5	N/A
Spain	0	3,015,902	0	3	9047.706
Sweden	0	1,406,271	0	6	8437.626
Iceland	N/A	N/A	N/A	3	N/A
Liechtenstein	N/A	N/A	N/A	0	N/A
Norway	0	1,309,390	0	7	9165.73
Total EU	2979	29851502	21879		85,496.78
Total EEA	2979	31160892	21879		94,662.51

Measure 1.2	
QRE 1.2.1	<p>We do not currently offer ad revenue sharing for creators in the EEA.</p> <p>We offer creator monetisation opportunities such as the TikTok Creator Fund (which was live during the reporting period but which has since been replaced with the Creator Rewards Program). These programs offer creators meeting certain eligibility criteria the opportunity to monetise their content based on a range of factors including, for example, the level of user interaction with the videos they post.</p>



	<p>All creators must comply with TikTok’s Community Guidelines (CGs), including our Integrity and Authenticity (I&A) policies. Where creators fail to comply with our CGs, this may result in loss of access to monetisation and / or loss of account access. Users in all EU Member States are notified by an in-app notification in their relevant local language where there has been a restriction of their ability to monetise, restriction of their access to a feature, removal or other restriction of access to their content, or a ban of their account.</p> <p>We prohibit accounts verified as belonging to a government, politician or political party from accessing monetisation features. They will, for instance, be ineligible for participation in content monetisation programs such as our Creator Fund (now replaced with the Creator Rewards Program). Along with our existing ban on political advertising, this means that accounts belonging to governments, politicians or political parties, will not be able to give or receive money through TikTok’s monetisation features, or spend money promoting their content (although exemptions are made for governments in certain circumstances such as for public health).</p>			
SLI 1.2.1	<p>Methodology of data measurement:</p> <p>Our I&A policies within our CGs are the first line of defence in combating harmful misinformation and deceptive behaviours on our platform. All creators are required to comply with our CGs, which set out the circumstances where we will remove, or otherwise limit the availability of, content.</p> <p>TikTok’s Creator Fund and the Creator Rewards Program do not relate to advertising and we do not currently offer ad revenue sharing to creators in the EEA. Creators who breach the CGs or Terms of Service are not eligible to receive rewards. We have set out the number of ads that have been removed from our platform for violation of our Covid-19 misinformation, and political content policies, as well our four new, more granular policies on medical misinformation, dangerous misinformation, manipulated media and dangerous conspiracy theories in SLI 1.1.1. Further, SLI 1.1.2 aims to provide an estimate of the potential impact on revenue of demonetising disinformation.</p> <p>We are working towards being able to provide more data for this SLI.</p>			
Member States	N/A	N/A	N/A	N/A
Total EU				
Total EEA				

Measure 1.3	
--------------------	--



<p>QRE 1.3.1</p>	<p>We partner with a number of industry leaders to provide a number of controls and transparency tools to advertising buyers with regard to the placement of ads.</p> <p>Controls: We offer pre-campaign solutions to advertisers so they can put additional safeguards in place before their campaign goes live to mitigate the risk of their advertising being displayed adjacent to certain types of user-generated content. These measures are in addition to the Community Guidelines (CGs), which provide overarching rules around the types of content that can appear on TikTok and are eligible for the For You feed:</p> <ul style="list-style-type: none"> • TikTok Inventory Filter: This is our proprietary system which enables advertisers to choose the profile of content they want their ads to run adjacent to. The Inventory Filter is now available in 18 jurisdictions in the EEA and is embedded directly in TikTok Ads Manager, the system through which advertisers purchase ads. More details can be found here. The Inventory Filter is informed by the GARM Framework and policies include topics which may be susceptible to disinformation. • TikTok Brand Safety by Integral Ad Science (IAS): Advertisers can select IAS (available in France and Germany) within the platform to ensure their ads run adjacent to content verified by IAS. IAS verifies content against the GARM Framework. Some disinformation content may be filtered by IAS as a result of the existing GARM Brand Safety Floor & Brand Suitability Framework categories, such as Sensitive Social Issues. <p>Transparency: We have partnered with third parties to offer post-campaign solutions that enable advertisers to assess the suitability of user-generated content that ran immediately adjacent to their ad in the For You feed, against their chosen brand suitability parameters:</p> <ul style="list-style-type: none"> • Zefr: Through our partnership with Zefr, advertisers can obtain campaign insights into brand suitability and safety on the platform. Zefr aligns with the GARM Framework. • IAS: Advertisers can measure brand safety, viewability and invalid traffic on the platform with the IAS Signal platform. As with IAS’s pre-bid solution covered above, this aligns with the GARM Framework. • DoubleVerify: We are partnering with DoubleVerify to provide advertisers with media quality measurement for ads. DoubleVerify is working actively with us to expand their suite of brand suitability and media quality solutions on the platform.
<p>Measure 1.4</p>	



<p>QRE 1.4.1</p>	<p>When TikTok advertises, we buy advertising space through ad networks (either directly or through agencies) which make available to us robust and reputable brand safety tools, which mitigate the risk of TikTok ads appearing next to sources of disinformation.</p> <p>As well as making IAS available on the platform, we make use of IAS to ensure our own ads run on or near suitable content. Using GARM standards, IAS reports on content which has been filtered or flagged and allows us to make changes to the context filters to avoid ads appearing next to similar content in the future by activating pre- and post-impression blocks towards unsafe content, themes and keywords.</p> <p>We monitor the placement of our ads closely (especially in the context of politically sensitive events such as the Ukraine War and Israel / Hamas conflict) and in the event our ads are found to run adjacent to or on sources of disinformation, we will investigate to determine whether the content in question has been correctly identified and verify this with IAS or GARM as appropriate. We will then adjust any filters or add the publication in question to a blocklist to prevent a recurrence.</p>
<p>Measure 1.5</p>	
<p>QRE 1.5.1</p>	<p>We have achieved the TAG Brand Safety Certified seal and the TAG Certified Against Fraud seal by the Trustworthy Accountability Group (TAG) in the EEA and globally. This required appropriate verification by external auditors. Details of our TAG seal can be found by searching for “TikTok” on their public register which can be found here.</p> <p>We have been certified by the Interactive Advertising Bureau (IAB) for the IAB Ireland Gold Standard 2.1 (listed here) and IAB Sweden Gold Standard 1.0 (listed here).</p>
<p>QRE 1.5.2</p>	<p>We have achieved the TAG Brand Safety Certified and TAG Certified Against Fraud seals and the IAB Ireland Gold Standard and IAB Sweden Gold Standard 1.0.</p>
<p>Measure 1.6</p>	
<p>QRE 1.6.1</p>	<p>We offer a variety of brand safety tools for preventing ads from being placed beside specific types of content. We continue to invest in our existing partnerships with leading third party brand safety and suitability providers (including DoubleVerify, IAS, and Zefr).</p> <p>We evaluate, on an ongoing basis, whether there are potential new partnerships, including with researchers, that may be appropriate for our platform. Furthermore, our ad policies help to ensure that the categories of content which are most likely to require such checks and integration of information do not make it onto the platform in the first place.</p>



QRE 1.6.2	We only purchase ads through ad networks which make robust and reputable brand safety tools available to us. All of our media investment is therefore protected by such tools.
QRE 1.6.3	We have partnered with several third parties (IAS, Double Verify and Zefr) to offer post-campaign solutions that enable advertisers to assess the suitability of user content that ran immediately adjacent to their ad in the For You feed.
QRE 1.6.4	Not applicable as TikTok does not rate sources.
SLI 1.6.1	N/A
	N/A
Data	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.

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].

- Launched four new ad policies in the EEA, which are aligned with our existing policies but provide increased granularity. The new policies cover:
 - Medical Misinformation
 - Dangerous Misinformation
 - Manipulated Media
 - Dangerous Conspiracy Theories



<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]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> Continuing to explore whether we should develop further policies targeted at specific types of harmful misinformation to increase the granularity of our ad policies. Globalising the implementation and improving enforcement of our four new harmful misinformation ad policies.
<p>Measure 2.1</p>	
<p>QRE 2.1.1</p>	<p>Paid ads are subject to our ad policies, which specifically prohibit misleading, inauthentic and deceptive behaviours. All ads are reviewed against these policies before being allowed on our platform. In order to improve our existing ad policies, we launched four new more granular ad policies in the EEA in July (covering Medical Misinformation, Dangerous Misinformation, Manipulated Media and Dangerous Conspiracy Theories) which advertisers also need to comply with.</p>
<p>SLI 2.1.1 – Numbers by actions enforcing policies above</p>	<p>Methodology of data measurement:</p> <p>We have set out the number of ads that have been removed from our platform for violation of our Covid-19 misinformation and political content policies, as well as our four new, more granular policies on medical misinformation, dangerous misinformation, manipulated media and dangerous conspiracy theories.</p> <p>The majority of ads that violate our newly launched misinformation policies, would have been removed under our existing policies. In cases where an ad is deemed violative for other policies and also of these additional misinformation policies, the removal is counted under the older policy. Therefore, the third column below shows only the number of ads removed where the sole reason was one of these four additional misinformation policies, and does not include ads already removed under our existing policies or where misinformation policies were not the driving factor for the removal.</p> <p>The data below suggests that our existing policies (such as political content and Covid-19 misinformation policies, in addition to other policy areas such as our inaccurate, misleading, or false content policy) already cover the majority of harmful misinformation ads, due to their expansive coverage.</p> <p>Note that numbers have only been provided for monetised markets and are based on where the ads were displayed.</p>



	Number of ad removals under the Covid-19 misinformation ad policy	Number of ad removals under the political content ad policy	Number of ad removals under the additional misinformation ad policies
Member States			
Austria	0	45	0
Belgium	0	51	0
Bulgaria	N/A	N/A	N/A
Croatia	N/A	N/A	N/A
Cyprus	N/A	N/A	N/A
Czech Republic	0	18	0
Denmark	0	27	0
Estonia	N/A	N/A	N/A
Finland	0	16	0
France	0	140	0
Germany	1	272	1



Greece	0	0	0
Hungary	0	50	0
Ireland	0	33	0
Italy	0	94	0
Latvia	N/A	N/A	N/A
Lithuania	N/A	N/A	N/A
Luxembourg	0	0	0
Malta	N/A	N/A	N/A
Netherlands	0	62	7
Poland	1	163	0
Portugal	0	16	0
Romania	0	134	0
Slovakia	N/A	N/A	N/A
Slovenia	N/A	N/A	N/A



Spain	1	118	1
Sweden	0	33	0
Iceland	N/A	N/A	N/A
Liechtenstein	N/A	N/A	N/A
Norway	0	37	0
Total EU	3	1272	9
Total EEA	3	1309	9

Measure 2.2	
QRE 2.2.1	<p>In order to identify content and sources that breach our ad policies, all ads go through moderation prior to going “live” on the platform.</p> <p>After the ad goes live on the platform, users can report any concerns using the “report” button, and the ad will be reviewed again and appropriate action taken if necessary.</p> <p>TikTok also operates a "recall" process whereby ads already on TikTok will go through an additional stage of review if certain conditions are met, including reaching certain impression thresholds. TikTok also conducts additional reviews on random samples of ads to ensure its processes are functioning as expected.</p>
Measure 2.3	
QRE 2.3.1	<p>In order to identify content and sources that breach our ad policies, all ads go through moderation prior to going “live” on the platform.</p>



	<p>After the ad goes live on the platform, users can report any concerns using the “report” button, and the ad will be reviewed again and appropriate action taken if necessary.</p> <p>TikTok also operates a "recall" process whereby ads already on TikTok will go through an additional stage of review if certain conditions are met, including reaching certain impression thresholds. TikTok also conducts additional reviews on random samples of ads to ensure its processes are functioning as expected.</p>					
SLI 2.3.1	<p>We are pleased to be able to report on the ads removed for breach of our Covid-19 misinformation and political content policies, as well as our new, more granular misinformation ad policies, including the impressions of those ads in this report.</p>					
	Number of ad removals under the Covid-19 misinformation ad policy	Number of ad removals under the political content ad policy	Number of ad removals under the additional more granular misinformation ad policies	Number of impressions for ads removed under the Covid-19 misinformation ad policy	Number of impressions for ads removed under the political content ad policy	Number of impressions for ads removed under the additional more granular misinformation ad policies
Member States						
Austria	0	45	0	0	397,478	2,808
Belgium	0	51	0	0	3,222,659	0
Bulgaria	N/A	N/A	N/A	N/A	N/A	N/A
Croatia	N/A	N/A	N/A	N/A	N/A	N/A
Cyprus	N/A	N/A	N/A	N/A	N/A	N/A
Czech Republic	0	18	0	0	238,887	0
Denmark	0	27	0	0	415,632	0
Estonia	N/A	N/A	N/A	N/A	N/A	N/A
Finland	0	16	0	0	1,047,991	1,030



France	0	140	0	0	2,784,405	3,518
Germany	1	272	1	0	3,661,928	1,935
Greece	0	0	0	0	0	0
Hungary	0	50	0	0	1,038,921	5,850
Ireland	0	33	0	0	391,170	0
Italy	0	94	0	0	3,619,351	5,931
Latvia	N/A	N/A	N/A	N/A	N/A	N/A
Lithuania	N/A	N/A	N/A	N/A	N/A	N/A
Luxembourg	0	0	0	0	0	0
Malta	N/A	N/A	N/A	N/A	N/A	N/A
Netherlands	0	62	7	0	842,172	601
Poland	1	163	0	0	4,958,443	206
Portugal	0	16	0	0	271,334	0
Romania	0	134	0	2,979	2,538,958	0
Slovakia	N/A	N/A	N/A	N/A	N/A	N/A
Slovenia	N/A	N/A	N/A	N/A	N/A	N/A
Spain	1	118	1	0	3,015,902	0
Sweden	0	33	0	0	1,406,271	0
Iceland	N/A	N/A	N/A	N/A	N/A	N/A
Liechtenstein	N/A	N/A	N/A	N/A	N/A	N/A



Norway	0	37	0	0	1,309,390	0
Total EU	3	1272	9	2979	29851502	21879
Total EEA	3	1309	9	2979	31160892	21879

Measure 2.4				
QRE 2.4.1	<p>We are clear with advertisers that their ads must comply with our ad policies (see TikTok Business Help Center). We explain that all ads are reviewed before being uploaded on our platform - usually within 24 hours. Where an advertiser has violated an ad policy they are informed by way of a notification. This is visible in their TikTok Ads Manager account or, where an advertiser has booked their ad through a TikTok representative, then the representative will inform the advertiser of any violations. Advertisers are able to make use of functionality to appeal rejections of their ads in certain circumstances. Ads already on TikTok may go through an additional stage of review if they are reported, if certain conditions are met (e.g., reaching certain impression thresholds) or because of random sampling conducted at TikTok’s own initiative.</p>			
SLI 2.4.1	<p>We are pleased to be able to share the number of appeals for ads removed under our Covid-19 misinformation and political content ad policies in this report. There were no appeals for ads removed under our new, more granular misinformation ad policies (and therefore no overturns either).</p>			
	Number of appeals for ads removed under the covid 19 policy	Number of appeals for ads removed under political content policy	Number of overturns of appeals under the covid 19 policy	Number of overturns of appeal under political content policy
Member States				
Austria	0	34	0	19
Belgium	0	21	0	11
Bulgaria	N/A	N/A	N/A	N/A
Croatia	N/A	N/A	N/A	N/A
Cyprus	N/A	N/A	N/A	N/A



Czech Republic	0	20	0	8
Denmark	0	19	0	9
Estonia	N/A	N/A	N/A	N/A
Finland	0	12	0	7
France	0	103	0	63
Germany	1	113	0	72
Greece	0	0	0	0
Hungary	0	17	0	10
Ireland	0	20	0	13
Italy	0	40	0	16
Latvia	N/A	N/A	N/A	N/A
Lithuania	N/A	N/A	N/A	N/A
Luxembourg	0	0	0	0
Malta	N/A	N/A	N/A	N/A
Netherlands	0	24	0	17
Poland	0	46	0	11
Portugal	0	12	0	8
Romania	0	60	0	50
Slovakia	N/A	N/A	N/A	N/A
Slovenia	N/A	N/A	N/A	N/A



Spain	0	43	0	18
Sweden	0	28	0	18
Iceland	N/A	N/A	N/A	N/A
Liechtenstein	N/A	N/A	N/A	N/A
Norway	0	18	0	13
Total EU	1	381	0	247
Total EEA	1	399	0	260

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.

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].	<ul style="list-style-type: none"> Continued to regularly participate in the working group on Ad Scrutiny. Sponsored the Global Fact 10 Global Fact-Checking Conference hosted by the International Fact-Checking Network at the end of June 2023 and hosted a panel discussion on our approach to countering harmful misinformation.
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



<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> • Continuing our engagement with relevant players such as GARM, IAB Sweden and IAB Ireland. • Exploring potential new partnerships with other organisations in order to increase the effectiveness of the scrutiny of ads placements. • Attending the Global Fact 11 Global Fact-Checking Conference hosted by the International Fact-Checking Network in 2024.
<p>Measure 3.1</p>	
<p>QRE 3.1.1</p>	<p>As set out later on in this report, we cooperate with a number of third parties to facilitate the flow of information that may be relevant for tackling purveyors of harmful misinformation. This information is shared internally to help ensure consistency of approach across our platform.</p> <p>At the end of June 2023, TikTok sponsored and presented at GlobalFact 10 2023 a fact checking summit hosted by the International Fact-Checking Network (IFCN). We look forward to attending again in 2024.</p> <p>We also continue to be actively involved in the Task-force working group for Chapter 2, working with other signatories to define and outline metrics regarding the monetary reach and impact of harmful misinformation. We are in close collaboration with industry to ensure alignment and clarity on the reporting of these code requirements.</p>
<p>Measure 3.2</p>	
<p>QRE 3.2.1</p>	<p>As a GARM member, together with our fellow members and signatories, we are committed to removing harmful misinformation from monetisation as part of our commitment to upholding the GARM Framework. The misinformation guidelines have been developed in coordination with the European Commission and in consultation with NGO partners, such as Consumers International and Reporters without Borders. We work with other GARM members to discuss relevant topics, including in a monthly GARM community call. We are engaged with GARM at a local level as well as globally. For example, we are a member of the GARM Nordics working committee.</p> <p>We work closely with IAB Sweden, IAB Ireland and other organisations such as TAG in the EEA and globally. We are also on the board of the Brand Safety Institute.</p> <p>We continue to share relevant insights and metrics within our quarterly transparency reports, which aim to inform industry peers and the research community. We continue to engage in the sub groups set up for insights sharing between signatories and the Commission.</p>



Measure 3.3	
QRE 3.3.1	We continue to work closely with GARM, IAB Sweden, IAB Ireland and other organisations such as TAG in the EEA and globally.



III. Political Advertising Commitments 4 - 13



III. Political Advertising	
Commitment 4	
Relevant Signatories commit to adopt a common definition of “political and issue 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]	Yes
If yes, list these implementation measures here [short bullet points].	<ul style="list-style-type: none"> • We co-chair the election working group and have been working with the other Signatories as part of this.
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]	<ul style="list-style-type: none"> • We are keeping developments in the regulatory landscape under review and will carefully consider whether we need to implement any measures as a result of the changes.
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 4.1	
Measure 4.2	
QRE 4.1.1 (for measures 4.1 and 4.2)	<p>We prohibit political advertising, which is acknowledged to be a potential source of disinformation, with this Code dedicating a full Chapter to the topic of Political Advertising. Specifically, per our ad policies, we do not allow political actors to place advertising, nor do we allow ads and landing pages which:</p> <ul style="list-style-type: none"> • reference, promote, or oppose candidates or nominees for public office, political parties, or elected or appointed government officials; • reference an election, including voter registration, voter turnout, and appeals for votes;



	<ul style="list-style-type: none"> include advocacy for or against past, current, or proposed referenda, ballot measures, and legislative, judicial, or regulatory outcomes or processes (including those that promote or attack government policies or track records); and reference, promote, or sell, merchandise that features prohibited individuals, entities, or content, including campaign slogans, symbols, or logos. <p>We do allow cause-based advertising and public services advertising from government agencies, non-profits and other entities if they are not driven by partisan political motives. Sharing political beliefs and engaging in political conversation is allowed as organic content, but our policies prohibit users from paying to advertise or promote this content.</p> <p>We also prohibit political content in branded content i.e. content which has been incentivised by a third party and needs to be disclosed in accordance with local advertising and consumer laws.</p> <p>We have been monitoring the development of the EU regulation on the transparency and targeting of political advertising (PAR) during and after the reporting period. We expect it will be published in the Official Journal of the European Union soon after publication of this report. We are carefully considering any potential impact the PAR might have on our policies and systems.</p>
QRE 4.1.2 (for measures 4.1 and 4.2)	Not applicable at this stage.

<h3 style="text-align: center;">III. Political Advertising</h3>	
<h4 style="text-align: center;">Commitment 5</h4> <p style="text-align: center;">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.</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]	No
If yes, list these implementation measures here [short bullet points].	N/A



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]	<ul style="list-style-type: none"> We are keeping developments in the regulatory landscape under review and will carefully consider whether we need to implement any measures as a result of the changes.
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 5.1	
QRE 5.1.1	Not applicable as TikTok does not allow political advertising, as outlined in our Political and issue-based advertising policy .

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	
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].	N/A
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]	We are keeping developments in the regulatory landscape under review and will carefully consider whether we need to implement any measures as a result of the changes.



If yes, which further implementation measures do you plan to put in place in the next 6 months?		N/A	
Measure 6.1			
QRE 6.1.1	Not applicable as TikTok does not allow political advertising.		
Measure 6.2			
QRE 6.2.1	TikTok prohibits political ads on the platform. For ads which are permitted, we provide enhanced information accessible through our “About this Ad” functionality , which was refined and enhanced during 2023 in order to ensure compliance with our transparency obligations under Article 26(1) of the Digital Services Act. This feature displays information including who has presented and paid for the ad, the parameters used to determine why the user has received the ad and about how to change those parameters.		
QRE 6.2.2	Not applicable as TikTok does not allow political advertising.		
SLI 6.2.1 – numbers for actions enforcing policies above	N/A		
Member States	N/A	N/A	N/A
Total EU			
Total EEA			

Measure 6.3			
QRE 6.3.1	Not applicable as TikTok does not allow political advertising.		
Measure 6.4			



QRE 6.4.1	Not applicable as TikTok does not allow political advertising.
Measure 6.5	
QRE 6.5.1	Not committed. This commitment is not applicable as TikTok is not a messaging app.

III. Political Advertising	
Commitment 7	
<p>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.</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]	No
If yes, list these implementation measures here [short bullet points].	N/A
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]	We are keeping developments in the regulatory landscape under review and will carefully consider whether we need to implement any measures as a result of the changes.
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 7.1	



QRE 7.1.1	<p>Where accounts are designated as Government, Politician, and Political Party Accounts (GPPPA), those accounts are banned from placing ads on TikTok (with the exception of certain government entities) and from monetisation features. We publish the details of our GPPPA policy on our website, where we set out who we consider to be a GPPPA and the restrictions on those types of accounts.</p> <p>In the EU, we apply an internal label to accounts belonging to a government, politician, or political party. Once an account has been labelled in this manner, a number of policies will be applied that help prevent misuse of certain features e.g., access to advertising features and solicitation for campaign fundraising are not allowed.</p>		
SLI 7.1.1 – numbers for action enforcing policies above (comparable metrics as for S 6.2.1)	N/A		
Member States	N/A	N/A	

Total EU				
Total EEA				



Measure 7.2	
QRE 7.2.1	Not applicable as TikTok does not allow political advertising.
QRE 7.2.2	Not applicable as TikTok does not allow political advertising.
Measure 7.3	
QRE 7.3.1	Not applicable as TikTok does not allow political advertising.
QRE 7.3.2	Not applicable as TikTok does not allow political advertising.
Measure 7.4	
QRE 7.4.1	Not applicable as TikTok does not allow political advertising.

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.	
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].	N/A
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the	We are keeping developments in the regulatory landscape under review and will carefully consider whether we need to implement any measures as a result of the changes.



maturity of the implementation of this commitment? [Yes/No]	
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 8.1	
Measure 8.2	
QRE 8.2.1 (for measures 8.1 & 8.2)	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.	
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].	N/A
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]	We are keeping developments in the regulatory landscape under review and will carefully consider whether we need to implement any measures as a result of the changes.
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A



Measure 9.1	
Measure 9.2	
QRE 9.2.1 (for measures 9.1 & 9.2)	Not applicable as TikTok does not allow political advertising.

III. Political Advertising	
Commitment 10	
<p>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.</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].	<ul style="list-style-type: none"> • Completed the roll out of the Commercial Content Library in the EEA. • Expanded the scope of the Commercial Content API.
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?	<ul style="list-style-type: none"> • Continuing to explore ways to improve the accessibility and reliability of the Commercial Content Library for our growing user base.
Measure 10.1	



Measure 10.2	
QRE 10.2.1 (for measures 10.1 & 10.2)	<p>Whilst we do not consider this provision applies to TikTok, given that TikTok does not allow political ads, we have completed the roll out of the Commercial Content Library to comply with our obligations under the DSA. The Commercial Content Library is a searchable database with information about paid ads and ad metadata, such as the advertising creative, dates the ad ran, main parameters used for targeting (e.g. age, gender), number of people who were served the ad, and more. It also includes information about content that is commercial in nature and tagged with either a paid partnership label or promotional label, such as content that promotes a brand, product or service, but that is not a paid ad (learn more on our Help Center).</p>

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.”	
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].	<ul style="list-style-type: none"> • Completed the roll out of the Commercial Content Library in the EEA. • Expanded the scope of the Commercial Content API.
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



<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> Continuing to explore ways to improve the accessibility and reliability of the Commercial Content Library for our growing user base.
<p>Measure 11.1</p>	
<p>Measure 11.2</p>	
<p>Measure 11.3</p>	
<p>Measure 11.4</p>	
<p>QRE 11.1.1 (for measures 11.1-11.4)</p>	<p>Whilst we do not consider this provision applies to TikTok, given that TikTok bans political ads, we have completed the roll out of the Commercial Content API in the EEA, to comply with our obligations under the DSA. This had previously been tested with a limited number of researchers. We have built commercial content related APIs that include ads, ad and advertiser metadata, and targeting information. These APIs will allow the public and researchers to perform customised, advertiser name or keyword based searches on ads and other commercial content data that is stored in the Commercial Content Library.</p>
<p>QRE 11.4.1</p>	<p>We value feedback on where we can improve any of our APIs. We will continue to receive feedback from researchers on their use of the Research and Commercial Content APIs and to make updates to better support independent research and enhance transparency about TikTok content.</p>

<h3>III. Political Advertising</h3>
<h4>Commitment 12</h4>
<p>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.</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]	No
If yes, list these implementation measures here [short bullet points].	TikTok did not subscribe to this commitment. Commitment 12 and associated measures are applicable to Civil Society only.
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?	TikTok did not subscribe to this commitment. Commitment 12 and associated measures are applicable to Civil Society only.
Measure 12.1	
Measure 12.2	
Measure 12.3	
QRE 12.1.1 (for measures 12.1-12.3)	Commitment 12 and measures 12.1, 12.2 and 12.3 are applicable to Civil Society only.

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.



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].	N/A
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]	We are keeping developments in the regulatory landscape under review and will carefully consider whether we need to implement any measures as a result of the changes.
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 13.1	
Measure 13.2	
Measure 13.3	
QRE 13.1.1 (for measures 13.1-13.3)	Whilst we do not allow political advertising, we are committed to remaining engaged with all discussions being held through the Task-force and other fora to ensure our policies and processes remain current and emerging and novel threats are addressed in our policies and enforcement.



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



<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]</p>	<p>Yes</p>
<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> • Launched a new tool to enable creators to label AI-generated content that they share on our platform, as well as guidelines restating our policy on Synthetic and Manipulated Media on when such content should be clearly disclosed and how the tool should be used. • To increase transparency around AI-powered products, we have now made it easier for users to understand when a TikTok effect uses AI by explicitly including “AI” in the effect name and the corresponding effect label. We have also updated our guidelines for creators using Effect House, our development platform which empowers creators to generate augmented reality effects, to encourage them to do the same. • In accordance with our commitments as a launch partner for PAI Responsible Practices on Synthetic Media, we worked on a case study outlining how the Practices informed our policy making on synthetic media. In addition, representatives from our team attended a series of workshops on content provenance and watermarking organised by PAI, which was attended by representatives of peer platforms and media outlets. • Joined industry partners as a party to the “Tech Accord to Combat Deceptive Use of AI in 2024 Elections” which is a set of commitments to deploy technology countering harmful AI-generated content meant to deceive voters. • We continue to participate in relevant working groups, such as the Generative AI working group, which commenced in September 2023. • We have enhanced our ability to detect covert influence operations, through a dual-pronged strategy that focuses on enhancing detection efforts by integrating insights gained from extensive global investigations, as well as developing strategic partnerships with third-party intelligence providers to complement our existing in-house capabilities. We also consult with members of our Safety Advisory Council to gain insight into, and obtain advice on, our efforts to detect covert influence operations as we continually work to improve our efforts in this regard.



<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]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> • Continuing to strengthen how we enforce our policy on Synthetic and Manipulated Media and exploring new products and initiatives to help enhance our detection and enforcement capabilities in relation to our policy on Synthetic and Manipulated Media, including by developing a user education/outreach campaign. • Whilst we already have a number of policies in place which address hack and leak related threats, we are aiming to develop a more targeted policy in this area, with the aim of reducing the harms inflicted by the unauthorised disclosure of hacked materials on the individuals, communities and organisations that may be implicated or exposed by such disclosures. • As new deceptive behaviours emerge, we'll continue to evolve our response, strengthen enforcement capabilities and develop appropriate product and policy solutions. We are also proactively working to understand the impact of generative AI on platform integrity, to strengthen our internal capabilities to disrupt adversarial abuse by malign actors who seek to weaponize AI technologies.
<p>Measure 14.1</p>	



QRE 14.1.1

As well as our Integrity and Authenticity (**I&A**) policies in our Community Guidelines (**CGs**) which safeguard against harmful misinformation (see QRE 18.2.1), our I&A policies also expressly prohibit deceptive behaviours. Our policies on deceptive behaviours relate to the TTPs as follows:

TTPs which pertain to the creation of assets for the purpose of a disinformation campaign, and to ways to make these assets seem credible:

Creation of inauthentic accounts or botnets (which may include automated, partially automated, or non-automated accounts)

Our I&A policies which address **Spam and Deceptive Account Behaviours** expressly prohibit account behaviours that may spam or mislead our community. You can set up multiple accounts on TikTok to create different channels for authentic creative expression, but not for deceptive purposes.

We do not allow spam including:

- accounts that are operated in bulk, through unauthorised automation, or in order to distribute high-volume commercial content; and
- operating networks of accounts that represent similar entities or post similar content to lead others to specific locations (on or off-platform), such as other accounts, websites, and businesses.

We also do not allow impersonation including:

- Accounts that pose as another real person or entity, such as using someone’s name, biographical details, content, or image without disclosing it; or
- Presenting as a person or entity that does not exist (a fake persona) with a demonstrated intent to mislead others on the platform.

If we determine someone has engaged in any of these deceptive account behaviours, we will ban the account, and may ban any new accounts that are created by that person.

Use of fake / inauthentic reactions (e.g. likes, up votes, comments) and use of fake followers or subscribers

Our I&A policies which address **fake engagement** do not allow the trade of services that attempt to artificially increase engagement or deceive TikTok's recommendation system. We do not allow our users to:

- facilitate the trade of services that artificially increase engagement, such as selling followers or likes; or
- provide instructions on how to artificially increase engagement on TikTok.

If we become aware of accounts or content with inauthentically inflated metrics, we will remove the associated fake followers or likes. Content that tricks or manipulates others as a way to increase engagement metrics, such as "like-for-like" promises and false incentives for engaging with content is ineligible for our For You feed.

Creation of inauthentic pages, groups, chat groups, fora, or domains

TikTok does not have pages, groups, chat groups, fora or domains. This TTP is not relevant to our platform.

Account hijacking or Impersonation

As stated above, our policies prohibit **impersonation** which refers to accounts that pose as another real person or entity or present as a person or entity that does not exist (a fake persona) with a demonstrated intent to mislead others on the platform. Our users are not allowed to use someone else's name, biographical details, or profile picture in a misleading manner. In order to protect freedom of expression, we do allow accounts that are clearly parody, commentary, or fan-based, such as where the account name indicates that it is a fan, commentary, or parody account and not affiliated with the subject of the account.

We also have a number of policies that address account hijacking. Our privacy and security policies under our CGs expressly prohibit users from providing access to their account credentials to others or enable others to conduct activities against our CGs. We do not allow access to any part of TikTok through unauthorised methods; attempts to obtain sensitive, confidential, commercial, or personal information; or any abuse of the security, integrity, or reliability of our platform. We also provide practical [guidance](#) to users if they have concerns that their account may have been hacked.



TTPs which 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:

Deliberately targeting vulnerable recipients (e.g. via personalised advertising, location spoofing or obfuscation), 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), use of deceptive practices to deceive/manipulate platform algorithms, such as to create, amplify or hijack hashtags, data voids, filter bubbles, or echo chambers and coordinated mass reporting of non-violative opposing content or accounts.

We fight against CIOs as our policies prohibit attempts to sway public opinion while also misleading our systems or users about the identity, origin, approximate location, popularity or overall purpose.

Where our teams have a high degree of confidence that an account is engaged in inauthentic coordination of content creation or amplification, uses deceptive practices to deceive/manipulate platform algorithm or coordinated mass reporting of non-violative opposing content/accounts and is engaged in or is connected to networks we took down in the past as part of a CIO, it is removed from our Platform in accordance with our CIO policy.

When we investigate and remove these operations, we focus on behaviour and assessing linkages between accounts and techniques to determine if actors are engaging in a coordinated effort to mislead TikTok's systems or our community. In each case, we believe that the people behind these activities coordinate with one another to misrepresent who they are and what they are doing. We know that CIOs will continue to evolve in response to our detection and networks may attempt to re-establish a presence on our platform. We continue to iteratively research and evaluate complex deceptive behaviours on our platform and develop appropriate product and policy solutions as appropriate in the long term. We publish all of the CIO networks we identify and remove voluntarily within our transparency reports, [here](#).

Use “hack and leak” operation (which may or may not include doctored content)



	<p>Whilst we already have a number of policies in place which address hack and leak related threats, we are aiming to develop a more targeted policy in this area, with the aim of reducing the harms inflicted by the unauthorised disclosure of hacked materials on the individuals, communities and organisations that may be implicated or exposed by such disclosures.</p> <p>We also have a number of additional policies that address hack and leak related threats (some examples are below):</p> <ul style="list-style-type: none"> • Our CIO policy addresses use of leaked documents to sway public opinion as part of a wider operation • Our Synthetic and Manipulated Media Policy captures materials that has been digitally altered without an appropriate disclosure • Our harmful misinformation policies combats conspiracy theories related to unfolding events and dangerous misinformation • Our Trade of Regulated Goods and Services policy prohibits trading of hacked goods <p>Deceptive manipulated media (e.g. “deep fakes”, “cheap fakes”...)</p> <p>Our Synthetic and Manipulated Media Policy requires deceptive or synthetic media that shows realistic scenes must be clearly disclosed (see our newsroom post, here).</p> <p>For the purposes of our policy, synthetic media refers to content created or modified by AI technology. It includes highly realistic digitally-created (fake) content of real people, such as a video of a real person speaking but their words have been modified or changed.</p> <p>In accordance with our policy, we prohibit:</p> <ul style="list-style-type: none"> • Synthetic media showing realistic scenes that are not prominently disclosed or labelled in the video;
--	--

- Synthetic media that contains the likeness (visual or audio) of a real person, including: (1) a young person, (2) an adult private figure, and (3) an adult public figure when used for political or commercial endorsements, or if it violates any other policy; and
- Material that has been edited, spliced, or combined (such as video and audio) in a way that may mislead a person about real-world events.

Non-transparent compensated messages or promotions by influencers

Our [Terms of Service](#) and [Branded Content Policy](#) require users posting about a **brand or product in return for any payment or other incentive** to disclose their content by enabling the branded content toggle which we make available for users. We also provide functionality to enable users to report suspected undisclosed branded content which reminds the user who posted the suspected undisclosed branded content of our requirements and prompts them to turn the branded content toggle on if required. We have made this requirement even clearer to users in our **Commercial Disclosures and Paid Promotion** policy in our March 2023 CG refresh, by increasing the information around our policing of this policy and providing specific examples.



<p>QRE 14.1.2</p>	<p>At TikTok, we place considerable emphasis on proactive content moderation and use a combination of technology and safety professionals to detect and remove harmful misinformation (see QRE 18.1.1) and deceptive behaviours on our Platform, <i>before</i> it is reported to us by users or third parties.</p> <p>For instance, we take proactive measures to prevent inauthentic or spam accounts from being created. Thus, we have created and use detection models and rule engines that:</p> <ul style="list-style-type: none"> • prevent inauthentic accounts from being created based on malicious patterns; and • remove registered accounts based on certain signals (i.e., uncommon behaviour on the platform). <p>We also manually monitor user reports of inauthentic accounts in order to detect larger clusters or similar inauthentic behaviours.</p> <p>However, given the complex nature of the TTPs, human moderation is critical to success in this area and TikTok's moderation teams therefore play a key role assessing and addressing identified violations. We provide our moderation teams with detailed guidance on how to apply the Integrity and Authenticity (I&A) policies in our Community Guidelines (CGs), including providing case banks of harmful misinformation claims to support their moderation work, and allow them to route new or evolving content to our fact-checking partners for assessment.</p> <p>In addition, where content reaches certain levels of popularity in terms of the number of video views, it will be flagged for further review. Such review is undertaken given the extent of the content's dissemination and the increase in potential harm if the content is found to be in breach of our CGs including our I&A policies.</p> <p>We have also set up specifically-trained teams that are focused on investigating and detecting CIO on our Platform. When we investigate and remove these operations, we focus on behaviour and assessing linkages between accounts and techniques to determine if actors are engaging in a coordinated effort to mislead TikTok's systems or our community. In each case, we believe that the people behind these activities coordinate with one another to misrepresent who they are and what they are doing.</p>
<p>Measure 14.2</p>	



QRE 14.2.1

The implementation of our policies is ensured by different means, including specifically-designed tools (such as toggles to disclose branded content - see QRE 14.1.1) or human investigations to detect deceptive behaviours (for CIO activities - see QRE 14.1.2).

The implementation of these policies is also ensured through enforcement measures applied in all Member States.

Where our teams have a high degree of confidence that an account amounts to an **impersonation**, or is engaged in or is connected to networks we took down in the past as part of a CIO, it is removed from our Platform. Please note that in relation to CIO, we are only able to provide data for Q2 and Q3 2023. We are building and testing data infrastructure that can provide information requested at a high level of fidelity. Additionally, CIO investigations are highly resource heavy and require in-depth analysis to ensure high confidence in proposed actions.

Similarly, where our teams have a high degree of confidence that a specific content violates one of our TTPs-related policies (see QRE 14.1.1), such content is removed from TikTok.

Lastly, we may reduce the discoverability of some content, including by making videos ineligible for recommendation in the For You feed section of our Platform. This is, for example, the case for content that tricks or manipulates users in order to inauthentically increase followers, likes, or views.

SLI 14.2.1 – SLI 14.2.4



TTP OR ACTION1	<p>TTP No. 1: Creation of inauthentic accounts or botnets (which may include automated, partially automated, or non-automated accounts)</p> <p>Methodology of data measurement</p> <p>We have based the number of: (i) fake accounts removed; and (ii) followers of the fake accounts (identified at the time of removal of the fake account), on the country the fake account was last active in.</p> <p>We have updated our methodology to report the monthly average of fake accounts as a percentage of monthly active users, in order to better reflect TTPs related content in relation to overall content on the service.</p>												
	SLI 14.2.1			SLI 14.2.2				SLI 14.2.3			SLI 14.2.4		
		Nr of actions taken by type		Interaction/engagement before action							TTPs related content in relation to overall content on the service		
List actions per member states (see example table above)		Number of fake accounts removed		Number of followers of fake accounts identified at the time of removal							Monthly average of Fake accounts as a % of monthly active users		



Member States												
Austria		251,063		2,397,040								
Belgium		2,390,730		2,303,991								
Bulgaria		197,458		326,219								
Croatia		157,774		1,843,426								
Cyprus		12,947		429,346								
Czech Republic		7,357,631		1,324,010								
Denmark		92,528		2,032,974								
Estonia		57,913		874,006								
Finland		102,068		2,112,314								
France		11,597,402		13,598,155								
Germany		31,144,007		8,497,185								
Greece		92,985		579,189								
Hungary		202,926		411,597								
Ireland		404,609		687,819								
Italy		8,126,109		6,383,510								
Latvia		22,552		337,403								
Lithuania		51,788		1,327,375								
Luxembourg		25,873		409,304								



Malta		36,884		219,122								
Netherlands		552,509		2,197,637								
Poland		7,351,662		805,857								
Portugal		490,298		457,831								
Romania		71,881		1,420,132								
Slovakia		45,297		388,484								
Slovenia		18,704		364,934								
Spain		22,352,682		19,356,944								
Sweden		59,664		774,457								
Iceland		13,043		496,052								
Liechtenstein		7,139		3,113								
Norway		164,945		3,029,077								
Total EU		93,267,944		71,860,261						1.10%		
Total EEA		93,453,071		75,388,503								

TTP OR ACTION 2	<p>TTP no. 2: Use of fake / inauthentic reactions (e.g. likes, up votes, comments)</p> <p>Methodology of data measurement:</p> <p>We based the number of fake likes that we removed on the country of registration of the user. We also based the number of fake likes prevented on the country of registration of the user.</p>
------------------------	--



	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4
	Nr of actions taken by type	Interaction/ engagement before action		
List actions per member states (see example table above)	Number of fake likes removed	Number of fake likes prevented		
Austria	2,717,132	2,897,601		
Belgium	4,387,703	3,199,509		
Bulgaria	809,500	1,474,814		
Croatia	211,473	1,161,951		
Cyprus	718,598	675,174		
Czech Republic	723,732	31,048,989		



Denmark	1,376,209	895,274		
Estonia	90,847	614,304		
Finland	796,220	3,823,942		
France	16,349,101	63,789,626		
Germany	27,132,455	13,721,644,961		
Greece	2,034,276	4,346,579		
Hungary	970,602	1,006,472		
Ireland	1,078,796	1,718,643		
Italy	11,014,933	32,439,801		
Latvia	198,732	1,314,296		
Lithuania	258,601	835,820		
Luxembo urg	272,999	941,247		



Malta	202,555	567,717		
Netherlands	5,456,017	3,025,822,873		
Poland	2,300,848	34,039,857		
Portugal	1,410,739	2,766,909		
Romania	2,337,979	3,266,437		
Slovakia	249,732	1,215,358		
Slovenia	202,409	995,686		
Spain	7,491,126	36,917,864		
Sweden	4,571,259	4,413,576		
Iceland	75,353	274,072		
Liechtenstein	32,213	29,544		
Norway	1,432,633	2,419,083		



Total EU	95,364,573	16,983,835,280		
Total EEA	96,904,772	16,986,557,979		

TTP OR ACTION 3	TTP No. 3: Use of fake followers or subscribers Methodology of data measurement: We based the number of fake followers that we removed on the country of registration of the user. We also based the number of fake followers prevented on the country of registration of the user.			
	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4
	Nr of actions taken by type	Interaction/ engagement before action		
List actions per member states (see example table above)	Number of fake followers removed	Number of fake follows prevented		
Member States				



Austria	2,273,866	12,200,638		
Belgium	3,370,834	4,602,633		
Bulgaria	357,276	708,813		
Croatia	199,952	911,350		
Cyprus	274,900	617,502		
Czech Republic	928,851	88,773,130		
Denmark	765,604	1,321,040		
Estonia	165,821	962,629		
Finland	728,413	3,432,373		
France	20,930,165	118,823,026		
Germany	24,411,624	125,866,088		
Greece	886,161	2,618,076		



Hungary	353,577	2,738,279		
Ireland	567,814	1,830,037		
Italy	8,043,235	77,882,051		
Latvia	225,262	5,006,844		
Lithuania	349,003	7,846,202		
Luxembourg	251,917	2,653,268		
Malta	69,744	11,376,488		
Netherlands	5,398,617	15,503,737		
Poland	1,717,684	68,005,031		
Portugal	766,295	9,217,885		
Romania	2,236,070	2,691,689		
Slovakia	232,043	1,591,365		



Slovenia	114,979	349,744		
Spain	5,740,282	87,305,386		
Sweden	3,115,487	13,109,027		
Iceland	57,653	968,476		
Liechtenstein	2,164	115,978		
Norway	1,084,614	3,993,243		
Total EU	84,475,476	667,944,331		
Total EEA	85,619,907	673,022,028		

TTP OR ACTION 4	<p>TTP No. 4: Creation of inauthentic pages, groups, chat groups, fora, or domains</p> <p>TikTok does not have pages, groups, chat groups, fora or domains. This TTP is not relevant to our Platform.</p>
------------------------	--



TTP OR ACTION 5	TTP No. 5: Account hijacking or impersonation			
	<p>Methodology of data measurement:</p> <p>The number of accounts removed under our impersonation policy is based on the approximate location of the users. We have updated our methodology to report the monthly average of impersonation accounts as a percentage of monthly active users as it better reflects the relation of the TTPs related content to overall content on the service.</p>			
	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4
	Nr of actions taken by type			TTPs related content in relation to overall content on the service
Member States	Number of account banned under impersonation policy			Impersonation accounts as a % of monthly active users
List actions per member states (see example table above)				
Austria	171			
Belgium	404			
Bulgaria	158			
Croatia	17			
Cyprus	46			
Czech Republic	106			



Denmark	63			
Estonia	16			
Finland	88			
France	3,381			
Germany	1,944			
Greece	148			
Hungary	182			
Ireland	153			
Italy	850			
Latvia	16			
Lithuania	22			
Luxembourg	12			
Malta	1			
Netherlands	678			
Poland	740			
Portugal	118			
Romania	1,267			
Slovakia	43			
Slovenia	10			
Spain	1,156			



Sweden	240			
Iceland	20			
Liechtenstein	0			
Norway	153			
Total EU	12,030			0.0014%
Total EEA	12,203			

TTP OR ACTION 6	<p>TTP No. 6. Deliberately targeting vulnerable recipients (e.g. via personalised advertising, location spoofing or obfuscation)</p> <p>Methodology of data measurement:</p> <p>The number of CIO networks targeting countries relates to the Q2 and Q3 2023 period. We have categorised disrupted CIO networks by the country we assess that the network originated in. We have included any network which originated in Europe or that targeted one or more European countries. We publish all of the CIO networks we identify and remove within our transparency reports, here.</p> <p>The number of accounts linked to CIO networks identified and removed are based on the geographic location of network operation and technical and behavioural evidence from proprietary and open sources. The number of followers of CIO networks has been based on the number of accounts that followed any account within a network as of the date of that network's removal.</p>						
	SLI 14.2.1		SLI 14.2.2			SLI 14.2.3	SLI 14.2.4
Member States (Network origin)	Nr of instances of identified TTPs	Nr of actions taken by type	Interaction/engagement before action	Views/impressions after action	Interaction/engagement after action	Trends on targeted audiences	



Q2 2023							
Russia	588 accounts in the network	588 removed accounts	36,331 accounts followed an account within the network as at the date of removal	0	0	<p>We assess that this network operated from Russia and targeted Russian audiences in Russia, Netherlands, Romania, France and the UK.</p> <p>The individuals behind this network created inauthentic accounts and hyper-posted content in order to artificially amplify specific pro-Russia viewpoints in the context of the war in Ukraine, circumventing the regional TikTok ban in Russia.</p>	
Greece	69 accounts in the network	69 removed accounts	25,898 accounts followed an account within the network as at the date of removal	0	0	<p>We assess that this network operated from Greece and targeted a Greek audience.</p> <p>The individuals behind this network created inauthentic accounts and hyper-posted content, artificially amplifying specific narratives favourable to the political party “New Democracy” and critical of the opposition party “Syriza”, targeting Greek elections discourse.</p>	



Belgium	68 accounts in the network	68 removed accounts	61,379 accounts followed an account within the network as at the date of removal	0	0	<p>We assess that this network operated from Belgium and targeted a Turkish audience.</p> <p>The individuals behind this network created inauthentic accounts in order to artificially amplify content favorable to president Erdogan and Turkish military, along with content promoting a negative image of the Kurdistan Worker's party (PKK), targeting discourse about elections in Türkiye.</p>	
Q3 2023							
Russia	12,820 accounts in the network	12,820 removed accounts	847,760 accounts followed an account within the network as at the date of removal	0	0	<p>We assess that this network operated from Russia and targeted a European audience, including Germany and Ukraine.</p> <p>The individuals behind this network created a large number of inauthentic accounts in order to covertly amplify pro-Russian foreign policy viewpoints in Europe within the context of the war between Russia and Ukraine.</p>	



<p>China</p>	<p>636 accounts in the network</p>	<p>636 removed accounts</p>	<p>29,757 accounts followed an account within the network as at the date of removal</p>	<p>0</p>	<p>0</p>	<p>We assess that this network operated from China and targeted a global audience, including the US and Japan.</p> <p>The individuals behind this network created inauthentic accounts and posted across multiple social media platforms in order to artificially amplify pro-China narratives.</p>	
<p>Russia</p>	<p>133 accounts in the network</p>	<p>133 removed accounts</p>	<p>199,569 accounts followed an account within the network as at the date of removal</p>	<p>0</p>	<p>0</p>	<p>We assess that this network operated from Russia and targeted Russian and Ukrainian audiences, as well as the Russian speaking audience in Europe.</p> <p>The individuals behind this network created inauthentic accounts in order to artificially amplify pro-Russian narratives, targeting discourse about the ongoing war between Russia and Ukraine.</p>	



Slovakia	69 accounts in the network	69 removed accounts	2,154 accounts followed an account within the network as at the date of removal	0	0	<p>We assess that this network operated from Slovakia and targeted a Slovakian audience.</p> <p>The individuals behind this network created opaque accounts which engaged in inauthentic audience building methods in order to inauthentically amplify anti-EU, anti-NATO and pro-Russian content in Slovakia.</p>	
Russia	19 accounts in the network	19 removed accounts	217,008 accounts followed an account within the network as at the date of removal	0	0	<p>We assess that this network operated from Russia and targeted users from Germany, Italy, Turkey, Serbia, Czechia, Poland and Greece using local languages.</p> <p>The individuals behind this network created inauthentic accounts, including fictitious news agencies in order to artificially amplify pro-Russian narratives, targeting the ongoing war between Russia and Ukraine.</p>	



TTP OR ACTION 7	<p>TTP No. 7: Deploy deceptive manipulated media (e.g. “deep fakes”, “cheap fakes”...)</p> <p>We have recently launched our Synthetic and Manipulated Media Policy. We are not able to share meaningful metrics in this report.</p>
------------------------	--

TTP OR ACTION 8	<p>TTP No. 8: Use “hack and leak” operation (which may or may not include doctored content)</p> <p>While we already have a number of policies in place which address hack and leak related threats, we are developing a more targeted response for certain risks related to this area. As such, we do not have metrics to share in this report.</p>
------------------------	--

TTP OR ACTION 9	<p>TTP No. 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)</p> <p>We have provided data on the CIO networks that we have disrupted in the Q2 and Q3 2023 period under TTP No. 6.</p>
------------------------	---

TTP OR ACTION 10	<p>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</p> <p>We have provided data on the CIO networks that we have disrupted in the Q2 and Q3 2023 period under TTP No. 6.</p>
-------------------------	---



TTP OR ACTION 11	TTP No. 11. Non-transparent compensated messages or promotions by influencers			
	Methodology of data measurement: The branded content toggle allows users to self-disclose the existence of a commercial relationship. We have based the number of times the branded content toggle has been used on the approximate location of the users.			
	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4
	Nr of actions taken by type			
Member States				
List actions per member states (see example table above)	Number of times the branded content toggle has been used to disclose the existence of a commercial relationship			
Austria	201,726			
Belgium	409,239			
Bulgaria	210,894			
Croatia	81,518			
Cyprus	182,232			
Czech Republic	2,070,316			
Denmark	93,365			
Estonia	30,929			



Finland	1,701,661			
France	86,677			
Germany	2,441,591			
Greece	618,160			
Hungary	72,018			
Ireland	188,301			
Italy	102,502			
Latvia	3,285,911			
Lithuania	73,220			
Luxembourg	3,359,131			
Malta	50,137			
Netherlands	18,715			
Poland	492,378			
Portugal	918,018			
Romania	918,426			
Slovakia	636,527			
Slovenia	272,277			
Spain	29,223			
Sweden	73,184			
Iceland	0			



Liechtenstein	0			
Norway	117,900			
Total EU	18,618,276			
Total EEA	18,736,176			

TTP OR ACTION 12	TTP No. 12: Coordinated mass reporting of non-violative opposing content or accounts			
	We have provided data on the CIO networks that we have disrupted in the Q2 and Q3 2023 period under TTP No. 6.			
	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4
Member States				
List actions per member states (see example table above)				

Measure 14.3	
QRE 14.3.1	We engaged with the Integrity of Services working group to set up the first list of TTPs.



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.

<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]</p>	<p style="text-align: center;">Yes</p>
<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> ● Launched a new tool to enable creators to label AI-generated content that they share on our platform, as well as guidelines restating our policy on Synthetic and Manipulated Media on when such content should be clearly disclosed and how the tool should be used. ● To increase transparency around AI-powered products, we have now made it easier for users to understand when a TikTok effect uses AI by explicitly including “AI” in the effect name and the corresponding effect label. We have also updated our guidelines for creators using Effect House, our development platform which empowers creators to generate augmented reality effects, to encourage them to do the same. ● In accordance with our commitments as a launch partner for PAI Responsible Practices on Synthetic Media, we worked on a case study outlining how the Practices informed our policy making on synthetic media. In addition, representatives from our team attended a series of workshops on content provenance and watermarking organised by PAI, which was attended by representatives of peer platforms and media outlets. ● Joined industry partners as a party to the “Tech Accord to Combat Deceptive Use of AI in 2024 Elections” which is a set of commitments to deploy technology countering harmful AI-generated content meant to deceive voters.



	<ul style="list-style-type: none"> We continue to participate in relevant working groups, such as the Generative AI working group, which commenced in September 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]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> Continuing to strengthen how we enforce our Synthetic and Manipulated Media Policy and exploring new products and initiatives to help enhance our detection and enforcement capabilities in relation to our Synthetic and Manipulated Media Policy, including user education initiatives.
<p>Measure 15.1</p>	
<p>QRE 15.1.1</p>	<p>We have updated our Synthetic and Manipulated Media Policy to better address the use of content created or modified by AI technology on our platform (see our newsroom post, here). Under our Integrity and Authenticity (I&A) policies, we also prohibit other types of manipulated media that amount to harmful misinformation.</p> <p>While we welcome the creativity that new AI may unlock, in line with our updated policy, users must proactively disclose when their content is AI-generated or manipulated but shows realistic scenes (i.e. fake people, places or events that look like they are real). We launched an AI labelling tool in September 2023, which allows users to self-disclose AI-generated content when posting. When this has been turned on, a tag “Creator labelled as AI-generated” is displayed to users. Alternatively, this can be done through the use of a sticker or caption, such as ‘synthetic’, ‘fake’, ‘not real’, or ‘altered’.</p> <p>We do not allow:</p> <ul style="list-style-type: none"> synthetic media showing realistic scenes that are not prominently disclosed or labelled in the video, synthetic media content which contains the likeness (visual or audio) of a real person - including: a young person, an adult private figure, and an adult public figure when used for political or commercial endorsements, or if it violates any other policy, material that has been edited, spliced, or combined (such as video and audio) in a way that may mislead a person about real-world events.



	We are currently developing a user education/outreach campaign in relation to this policy and are exploring products and initiatives to enhance our detection and enforcement capabilities.
Measure 15.2	
QRE 15.2.1	<p>We have a number of measures to ensure the AI systems we develop uphold the principles of fairness and comply with applicable laws. To that end:</p> <ul style="list-style-type: none"> • We have in place internal guidelines and training to help ensure that the training and deployment of our AI systems comply with applicable data protection laws, as well as principles of fairness. • We have instituted a compliance review process for new AI systems that meet certain thresholds, and are working to prioritise review of previously developed algorithms. <p>We are proud to be a launch partner of the Partnership on AI's Responsible Practices for Synthetic Media. In accordance with our commitments as a launch partner, we worked on a case study outlining how the Practices informed our policy making on synthetic media. In addition, representatives from our team attended a series of workshops on content provenance and watermarking organised by PAI, which was attended by representatives of peer platforms and media outlets.</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.	
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



<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> Actively engaged with the Crisis Response working group, proactively sharing insights and learnings about relevant areas including CIOs. 		
<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]</p>	<p>Yes</p>		
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> Continuing to share relevant insights and metrics within our quarterly transparency reports, which aim to inform industry peers and the research community. Continuing to engage in the sub groups set up for insights sharing between signatories and the Commission. As new deceptive behaviours emerge, continuing to evolve our response, strengthen enforcement capabilities, develop appropriate product and policy solutions as appropriate. 		
<p>Measure 16.1</p>			
<p>QRE 16.1.1</p>	<p>Central to our strategy for identifying and removing CIO from our Platform, is working with our stakeholders from civil society to user reports. This approach facilitates us - and others - disrupting the network's operations in their early stages. In addition to continuously enhancing our in-house capabilities, we proactively engage in comprehensive reviews of our peers' publicly disclosed findings and implement necessary actions in alignment with our policies.</p> <p>We share relevant insights and metrics within our quarterly transparency reports, which aim to inform industry peers and the research community.</p> <p>We continue to engage in the sub groups set up for insights sharing between signatories and the Commission. We are engaged with GARM at a local and a global level.</p>		
<p>SLI 16.1.1 Numbers of actions as a result of information sharing</p>	<p>N/A</p>		



Data			
Measure 16.2			
QRE 16.2.1	We publish all of the CIO networks we identify and remove within our transparency reports here . As new deceptive behaviours emerge, we'll continue to evolve our response, strengthen enforcement capabilities, and publish our findings.		



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.

<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]</p>	<p>Yes</p>
---	------------



If yes, list these implementation measures here [short bullet points].

- Rolled out 11 new media literacy campaigns in Europe in collaboration with local media literacy bodies and our trusted fact-checking partners on topics identified as priority areas for increased digital literacy for our users in Europe. Of these media literacy campaigns:
 - Six (Austria, Bulgaria, Czech Republic, Croatia, Germany and Slovenia) were specific to the war in Ukraine, including identifying misinformation and manipulated media reports.
 - Five (Finland, Ireland, Italy, Spain and Sweden) were focused on general media literacy and critical thinking skills.
- Continued our extensive in-app interventions, including video tags, search interventions and in-app information centres, available in 23 official EU languages and Norwegian and Icelandic for EEA users, around the Israel-Hamas Conflict, Climate Change, Covid-19 and Covid-19 Vaccine, Holocaust Denial, Mpox and the War in Ukraine.
- Promoted election integrity in the run up to country-level EU elections in Spain, Slovakia, Poland and the Netherlands by:
 - Inviting regional experts to share their insights with our internal teams as part of our Election Speaker Series.
 - Launching additional in-app election campaigns, using our intervention tools to connect users to authoritative information sources.
 - Our in-app campaign for the Netherlands also included bespoke media literacy videos.
- Continued our detection and labelling of designated state-affiliated media in Europe and Asia and expanded the availability of state-controlled media labels to Sub-Saharan Africa, further increasing transparency for EU users.
- In keeping with our [Synthetic and Manipulated Media Policy](#):
 - Launched a new [AI-generated label](#) for creators to disclose content that is completely AI-generated or significantly edited by AI.
 - Began testing automated AI-generated content labels that we plan to apply automatically to content that we detect was edited or created with AI.
 - Introduced more clarity around AI-powered TikTok products by renaming TikTok AI effects to explicitly include "AI" in their name and corresponding effects label, and updated our guidelines for [Effect House creators](#) to do the same.



	<ul style="list-style-type: none"> • Advanced our commitment to sustainability and climate literacy at COP28 by launching a new \$1M initiative to tackle climate misinformation in support of Verified for Climate, a joint program of the United Nations and Purpose. Verified works with a range of civil society groups, media broadcasters, activists, and companies around the world to help deliver Verified information to millions of people. • To raise awareness and advocacy around sustainability and climate action, TikTok continued a global #ClimateAction campaign coinciding with the COP28 UN Climate Change Conference to encourage communities all over the world to join climate conversations and take action that has a positive impact on our planet. #ClimateAction has now garnered over 2 billion video views globally since the launch of the campaign at COP26. • TikTok continues to co-chair the working group on Elections.
<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]</p>	<p>Yes</p>



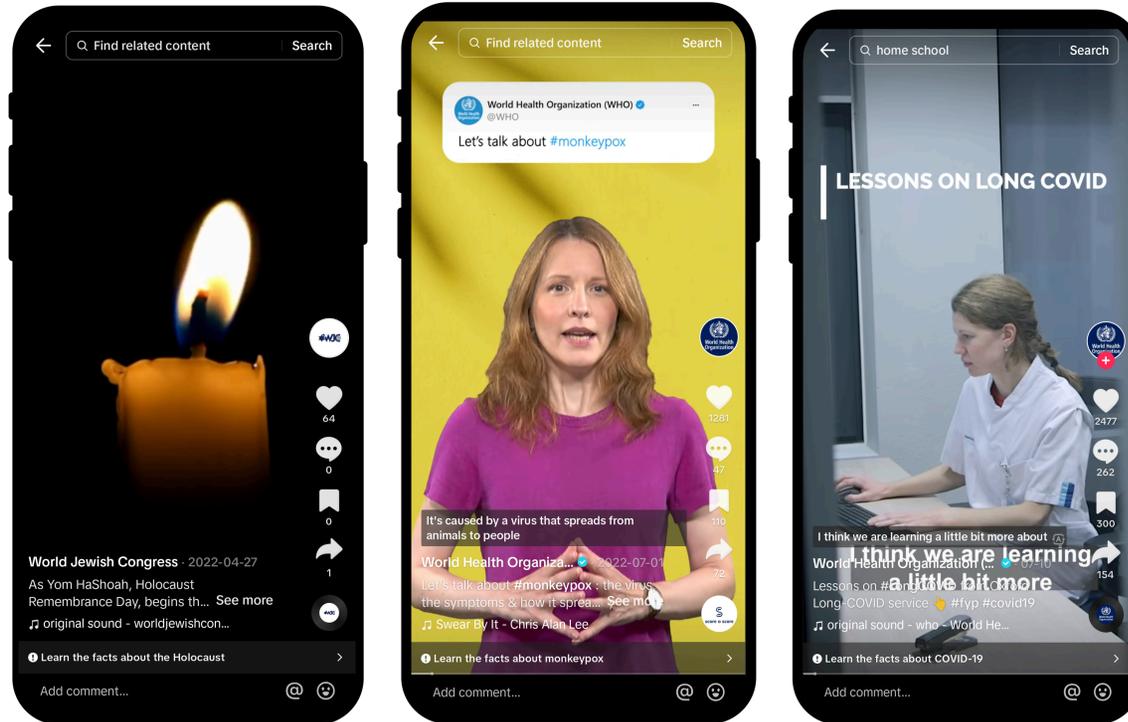
If yes, which further implementation measures do you plan to put in place in the next 6 months?

- Rolling out two media literacy campaigns in Europe in collaboration with our trusted fact-checking partners based on topics identified as priority areas for increased digital literacy of our users.
- Working toward localised media literacy activations in all 27 EU Member States by the end of 2024, with the majority being activated ahead of the European Parliamentary Elections in June 2024.
- Continuing to work with our fact-checking partners to identify local harmful misinformation trends in specific countries and develop tailored, localised media literacy campaigns to tackle such trends.
- Promoting election integrity in the run up to country-level EU elections by continuing to invite regional experts to share insights as part of our Election Speaker Series and launching additional in-app election campaigns to direct users to authoritative information.
- Expanding our user empowerment efforts through partnerships with expert organisations on key issues. For example, in Germany we will be partnering with Amadeu Antonio Stiftung on the Demo:create project, an educational project that will support some young TikTok users to effectively deal with hate speech, disinformation and misinformation on platforms.
- Continuing to invest in our detection capabilities of state-affiliated media accounts and to work with third party external experts to shape our state-affiliated media policy and assessment of state-controlled media labels.
- Continuing to enhance our AI generated content detection capabilities by:
 - Testing automated AI-generated content labels that we plan to apply automatically to content that we detect has been edited or created with AI.
 - Working with industry through content provenance partnerships.
- Progressing our partnership with [Verified for Climate](#) by bringing together a team of Verified Champions, including trusted messengers and experts from Brazil, the United Arab Emirates, Spain, and select TikTok creators, to tackle climate misinformation and disinformation while driving climate action within the TikTok community.
- Publishing a new page in our Transparency Center [Protecting the integrity of elections](#) and an updated article on [Combating harmful misinformation](#) to bring greater transparency about our integrity and authenticity efforts to our community.
- Publishing a new Misinformation Guide in our Safety Center.
- Building on our efforts to raise users' awareness about the credibility of content and to encourage people to reconsider sharing unverified content by expanding the application of our unverified content label to high risk and crisis events.



	<ul style="list-style-type: none"> Continuing to invest in training and development for our human moderation teams.
--	--

Measure 17.1	
QRE 17.1.1	<p>In addition to systematically removing content from our platform that violates our I&A policies, we continue to dedicate significant resources to expanding our in-app measures that show users additional context on certain content, redirecting them to authoritative information and making these tools available in 23 EU official languages (plus, for EEA users, Norwegian and Icelandic).</p> <p>We work with external experts to combat harmful misinformation. For example, the World Health Organisation (WHO) on medical information, and our global fact-checking partners, taking into account their feedback, as well as user feedback, to continually identify new topics and consider which tools may be best suited for raising awareness around that topic.</p> <p>Since 2020, on topics such as Climate Change, Covid-19, Covid-19 Vaccine, Holocaust Denial, MPox and the War in Ukraine, we have deployed a combination of in-app user intervention tools.</p> <p>Video notice tags. A video notice tag is an information bar at the bottom of a video which is automatically applied to a specific word or hashtag (or set of hashtags). The information bar is clickable and invites users to “<i>Learn more about [the topic]</i>”. Users will be directed to an in-app guide, or reliable third party resource, as appropriate.</p>



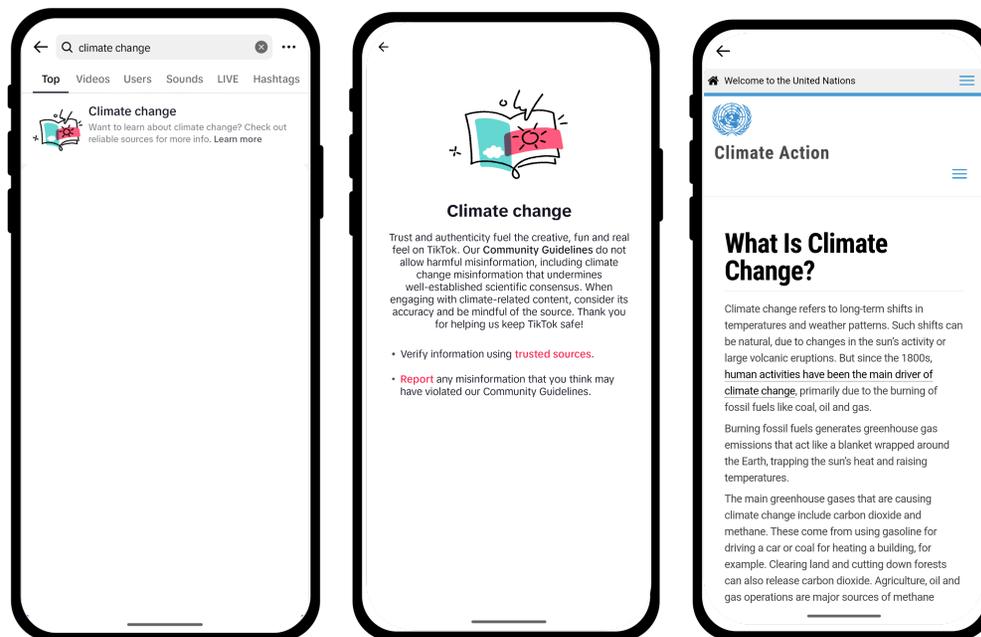
Holocaust Facts Video Notice Tag

Mpox Video Notice Tag

Covid-19 Video Notice Tag

Search intervention. If users search for terms associated with a topic, they will be presented with a banner which encourages them to verify the facts and provides them with a link to a trusted source of information. Search interventions are not deployed for search terms that violate our Community Guidelines, which are actioned according to our policies.

- For example, in April 2023, we launched a [climate change search intervention tool](#) in 23 official EU languages (plus Norwegian and Icelandic for EEA users), which redirects users looking for climate change-related content to authoritative information and encourages them to report any potential misinformation they see. We worked with the UN to source the authoritative information and redirect users to their [resources](#).



Public service announcement (PSA). If users search for a hashtag on the topic, they will be served with a public service announcement reminding them about our Community Guidelines and presenting them with links to a trusted source of information.

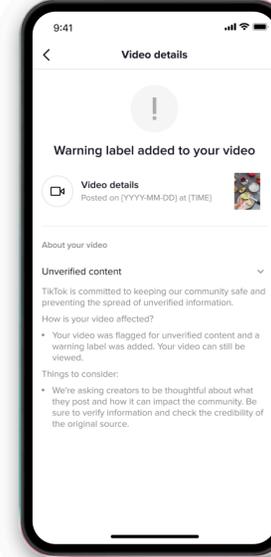
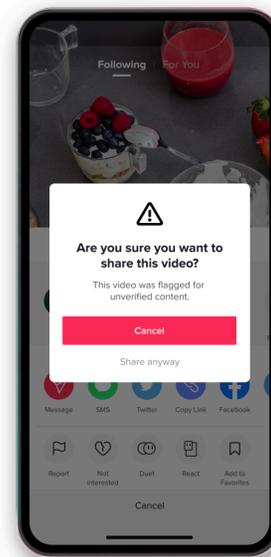
Unverified content label. In addition to the above mentioned tools, to encourage users to consider the reliability of content related to an emergency or unfolding event, which has been assessed by our fact-checkers but cannot be verified as accurate i.e., ‘unverified content’, we apply warning labels and prompt people to [reconsider sharing](#) such content. Details of these warning labels are included in our [Community Guidelines](#).

Where users continue to post despite the warning:

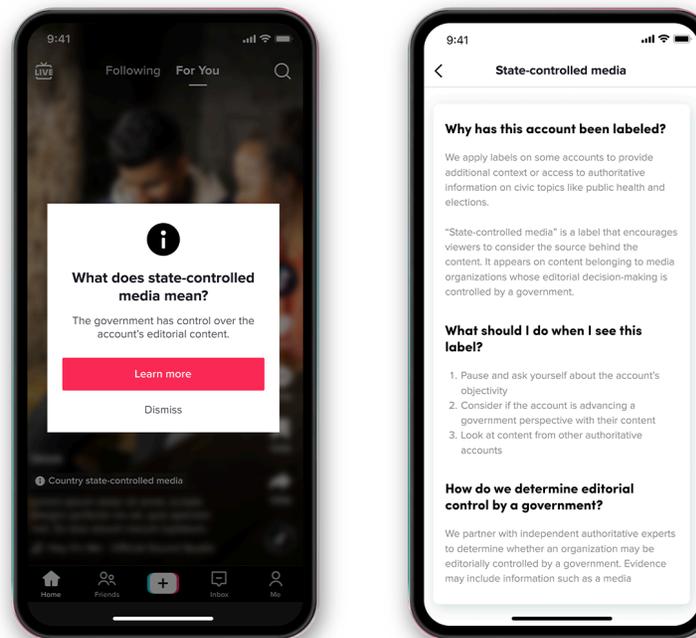
- To limit the spread of potentially misleading information, the video will become ineligible for recommendation in the For You feed.



- The video's creator is also notified that their video was flagged as unsubstantiated content and is provided additional information about why the warning label has been added to their content. Again, this is to raise the creator's awareness about the credibility of the content that they have shared.

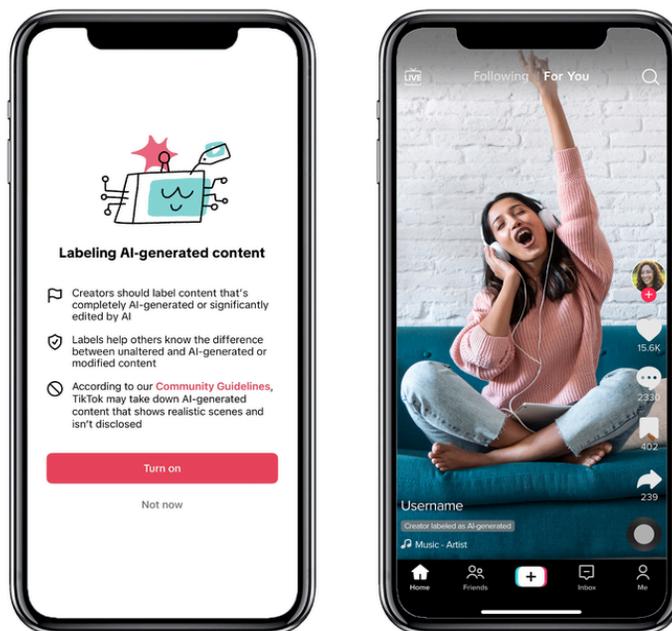


State-controlled media label. Our state-affiliated media policy is to label accounts run by entities whose editorial output or decision-making process is subject to control or influence by a government. We apply a prominent label to content and accounts from state-controlled media. The user is also shown a screen pop-up providing information about what the label means, inviting them to “learn more”, and redirecting them to an [in-app page](#). This measure brings transparency to our community, raises users’ awareness, and encourages users to consider the reliability of the source. We continue to work with experts to inform our approach and continue to expand its use, including most recently to Sub-Saharan Africa.



In the EU, Iceland and Liechtenstein, we have also taken steps to restrict access to content from Russia Today, Sputnik, Rossiya RTR / RTR Planeta, Rossiya 24 / Russia 24 and TV Centre International.

AI-generated content label. As more creators take advantage of Artificial Intelligence (AI) to enhance their creativity, we want to support transparent and responsible content creation practices. On 19 September 2023, TikTok launched a new AI-generated label for creators to disclose content that is completely AI-generated or significantly edited by AI, in keeping with our Synthetic and Manipulated Media Policy. In the interests of transparency, we have renamed TikTok AI effects to explicitly include "AI" in their name and corresponding effects label, and updated our guidelines for Effect House creators to do the same. The launch of this new tool to help creators label their AI-generated content was accompanied by a [creator education campaign](#), a [Help Center page](#), and a [Newsroom Post](#).



Dedicated online and in-app information resources. The above mentioned tools provide users with links to accurate and up-to-date information from trusted sources. Depending on the topic, or the relevant EU country, users may be directed to an external authoritative source (e.g., a national government website or an independent national electoral commission), an in-app information centre (e.g., War in Ukraine), or a dedicated page in the TikTok Safety Center or Transparency Center.

We use our [Safety Center](#) to inform our community about our approach to safety, privacy, and security on our platform. Relevant to combating harmful misinformation, we have dedicated information on:

- [Online challenges, Covid-19, Election integrity](#), and how to safely share content about [tragic events](#) on TikTok.
- Our [safety partners](#) page provides details of some of our work with global experts, non-governmental organisations, and industry associations to help build a safe platform for our community.

Users can learn more about our transparency efforts in our dedicated [Transparency Center](#), available in a number of EU languages, which houses our transparency reports, including the reports we have published under this Code, as well as



	<p>information on our commitments to maintaining platform integrity e.g., Protecting the integrity of elections, Combating misinformation and Countering influence operations.</p> <p>We also use Newsroom posts to keep our community informed about our most recent updates and efforts across <i>News</i>, <i>Product</i>, <i>Community</i>, <i>Safety</i> and <i>Product</i>. Users can filter posts by country (or by those applicable to the EU), to view regionally relevant posts and view posts in their preferred language where available. For example, upon publication of our second Code report in September 2023, we provided users with an overview of our efforts to build community resilience against harmful misinformation. We also updated users about our 2023 #ClimateAction campaign and new \$1M initiative to tackle climate misinformation in support of Verified for Climate.</p>		
<p>SLI 17.1.1 - actions enforcing policies above</p>	<p>Methodology of data measurement:</p> <p>The number of impressions, clicks and click through rates of video notice tags, search interventions and public service announcements are based on the approximate location of the users that engaged with the tools. The number of impressions of the Safety Center pages is based on the IP location of the users.</p> <p>For this reporting period, we are pleased to be able to report on engagement data for our state-controlled media label, applied in line with our state-affiliated media policy, and data for the climate change search intervention.</p>		
	<p>Total count of the tool's impressions</p>	<p>Interactions/ engagement with the tool</p>	<p>Other relevant metrics</p>
	<p>Number of impressions of the State-Controlled Media label</p>	<p>Number of clicks of the State-Controlled Media label</p>	<p>Numbers of clicks through rate of the State-Controlled Media label</p>
<p>Member States</p>			
<p>Austria</p>	<p>1,634,194</p>	<p>11,483</p>	<p>0.70%</p>
<p>Belgium</p>	<p>1,984,505</p>	<p>20,149</p>	<p>1.02%</p>
<p>Bulgaria</p>	<p>10,010,410</p>	<p>17,696</p>	<p>0.18%</p>
<p>Croatia</p>	<p>831,037</p>	<p>6,599</p>	<p>0.79%</p>
<p>Cyprus</p>	<p>417,560</p>	<p>1,560</p>	<p>0.37%</p>
<p>Czech Republic</p>	<p>1,087,871</p>	<p>10,886</p>	<p>1.00%</p>



Denmark	1,010,927	9,357	0.93%
Estonia	547,311	3,760	0.69%
Finland	1,163,094	30,450	2.62%
France	7,601,510	217,775	2.86%
Germany	15,163,315	99,615	0.66%
Greece	2,180,879	17,142	0.79%
Hungary	14,285,932	24,791	0.17%
Ireland	1,541,903	18,715	1.21%
Italy	8,791,546	118,606	1.35%
Latvia	1,665,791	4,993	0.30%
Lithuania	1,414,361	7,068	0.50%
Luxembourg	126,015	1,093	0.87%
Malta	241,648	784	0.32%
Netherlands	3,935,288	34,556	0.88%
Poland	110,377,745	156,916	0.14%
Portugal	851,398	10,967	1.29%
Romania	11,739,350	64,898	0.55%
Slovakia	887,848	4,497	0.51%
Slovenia	382,024	1,877	0.49%
Spain	4,397,084	27,082	0.62%



Sweden	2,472,670	23,481	0.95%
Iceland	149209	1049	0.70%
Liechtenstein	4846	40	0.83%
Norway	1,965,893	12,493	0.64%
Total EU	206743216	946796	0.46%
Total EEA	208863164	960378	0.46%

	Number of impressions of Video Notice Tag covered by Intervention (Covid-19)	Number of clicks of Video Notice Tag covered by Intervention (Covid-19)	Click Through Rate of Video Notice Tag covered by Intervention (Covid-19)
Member States			
Austria	18,373,468	29,120	0.16%
Belgium	14,172,823	27,849	0.20%
Bulgaria	5,881,748	12,026	0.20%
Croatia	3,626,973	6,499	0.18%
Cyprus	2,969,577	4,969	0.17%
Czech Republic	16,851,279	33,998	0.20%
Denmark	3,324,293	7,527	0.23%
Estonia	2,799,222	5,324	0.19%
Finland	11,817,233	21,926	0.19%



France	9,970,158	19,545	0.20%
Germany	184,022,260	257,260	0.14%
Greece	26,532,999	42,206	0.16%
Hungary	18,106,759	33,773	0.19%
Ireland	23,042,143	40,614	0.18%
Italy	218,862,766	430,747	0.20%
Latvia	6,368,419	10,587	0.17%
Lithuania	4,848,333	9,595	0.20%
Luxembourg	1,262,387	2,586	0.20%
Malta	1,302,681	2,175	0.17%
Netherlands	37,780,151	66,720	0.18%
Poland	65,687,631	104,361	0.16%
Portugal	18,701,901	42,626	0.23%
Romania	35,983,542	61,432	0.17%
Slovakia	3,929,976	7,426	0.19%
Slovenia	3,480,916	6,266	0.18%
Spain	133,847,810	286,174	0.21%
Sweden	25,348,002	59,180	0.23%



Iceland	1293583	2489	0.001924113
Liechtenstein	44086	126	0.00285805
Norway	5,395,002	12,389	0.23%
Total EU	898895450	1632511	0.18%
Total EEA	905628121	1647515	0.18%
	Number of impressions of Video Notice Tag covered by Intervention (Covid-19 Vaccine)	Number of clicks of Video Notice Tag covered by Intervention (Covid-19 Vaccine)	Click Through Rate of Video Notice Tag covered by Intervention (Covid-19 Vaccine)
Member States			
Austria	6,584,385	15,730	0.24%
Belgium	9,384,773	21,206	0.23%
Bulgaria	2,769,686	7,082	0.26%
Croatia	2,460,787	5,061	0.21%
Cyprus	796,853	1,847	0.23%
Czech Republic	3,510,594	8,577	0.24%
Denmark	4,088,996	11,881	0.29%
Estonia	722,001	1,754	0.24%
Finland	3,601,701	8,942	0.25%
France	66,032,536	145,910	0.22%



Germany	62,579,910	127,498	0.20%
Greece	7,038,692	15,529	0.22%
Hungary	5,075,626	10,033	0.20%
Ireland	8,674,845	20,379	0.23%
Italy	144,897,909	354,574	0.24%
Latvia	1,279,101	2,603	0.20%
Lithuania	1,534,675	3,666	0.24%
Luxembourg	598,642	1,600	0.27%
Malta	518,524	910	0.18%
Netherlands	14,936,228	35,108	0.24%
Poland	17,854,968	30,340	0.17%
Portugal	6,350,506	16,091	0.25%
Romania	10,557,174	22,854	0.22%
Slovakia	1,789,762	4,911	0.27%
Slovenia	1,137,914	2,586	0.23%
Spain	74,614,052	167,408	0.22%
Sweden	11,349,345	30,477	0.27%
Iceland	411,984	1268	0.31%



Liechtenstein	16,042	39	0.24%
Norway	5,247,079	14,227	0.27%
Total EU	470,740,185	1,074,557	0.23%
Total EEA	476,415,290	1,090,091	0.23%

	Number of impressions of Video Notice Tag covered by Intervention (Holocaust Misinformation/Denial)	Number of clicks of Video Notice Tag covered by Intervention (Holocaust Misinformation/Denial)	Click Through Rate of Video Notice Tag covered by Intervention (Holocaust Misinformation/Denial)
Member States			
Austria	4,210,704	11,732	0.28%
Belgium	8,838,533	35,043	0.40%
Bulgaria	1,016,575	4,351	0.43%
Croatia	1,085,006	3,873	0.36%
Cyprus	429,807	1,941	0.45%
Czech Republic	3,258,594	12,818	0.39%
Denmark	3,130,537	10,318	0.33%
Estonia	619,971	2,641	0.43%
Finland	3,945,577	16,810	0.43%
France	54,505,543	229,276	0.42%
Germany	37,173,924	92,689	0.25%



Greece	3,455,708	12,330	0.36%
Hungary	4,079,063	14,885	0.36%
Ireland	5,293,750	14,291	0.27%
Italy	16,598,913	49,493	0.30%
Latvia	677,528	2,826	0.42%
Lithuania	1,088,579	3,974	0.37%
Luxembourg	415,656	1,657	0.40%
Malta	283,181	842	0.30%
Netherlands	13,742,082	37,447	0.27%
Poland	21,228,164	62,768	0.30%
Portugal	2,754,773	11,791	0.43%
Romania	5,395,175	24,694	0.46%
Slovakia	859,312	2,959	0.34%
Slovenia	840,175	2,518	0.30%
Spain	13,047,858	56,370	0.43%
Sweden	7,618,198	30,781	0.40%
Iceland	387,502	1346	0.35%
Liechtenstein	10,370	27	0.26%



Norway	4,547,015	16,388	0.36%
Total EU	215,592,886	751118	0.35%
Total EEA	220,537,773	768879	0.35%
	Number of impressions of Video Notice Tag covered by Intervention (MPox)	Number of clicks of Video Notice Tag covered by Intervention (MPox)	Click Through Rate of Video Notice Tag covered by Intervention (MPox)
Member States			
Austria	118,848	224	0.19%
Belgium	105,748	271	0.26%
Bulgaria	84,996	184	0.22%
Croatia	38,423	96	0.25%
Cyprus	20,442	64	0.31%
Czech Republic	66,053	184	0.28%
Denmark	50,392	159	0.32%
Estonia	20,203	47	0.23%
Finland	21,213	86	0.41%
France	518,381	1,361	0.26%
Germany	2,124,168	3,072	0.14%
Greece	164,485	487	0.30%
Hungary	149,282	377	0.25%



Ireland	67,776	151	0.22%
Italy	854,196	1,750	0.20%
Latvia	33,933	69	0.20%
Lithuania	30,901	66	0.21%
Luxembourg	9,576	26	0.27%
Malta	11,178	35	0.31%
Netherlands	215,348	453	0.21%
Poland	359,460	749	0.21%
Portugal	359,947	2,110	0.59%
Romania	269,559	461	0.17%
Slovakia	17,470	33	0.19%
Slovenia	19,670	52	0.26%
Spain	804,121	1,784	0.22%
Sweden	42,849	148	0.35%
Iceland	5118	18	0.35%
Liechtenstein	182	2	1.10%
Norway	29,603	94	0.32%
Total EU	6,578,618	14499	0.22%



Total EEA	6,613,521	14613	0.22%
	Number of impressions of topic covered by video Intervention (Regional Elections)	Number of clicks by video Intervention (Election)	Number of CTR by video Intervention (Election)
Member States			
Netherlands	484,882,414	896,980	0.18%
Poland	974,623,710	1,241,253	0.13%
Slovakia	57,872,892	103,396	0.18%
Spain	37,703,002	68,098	0.18%
Total EU	1,555,082,018	2,309,727	0.15%
Total EEA	1,555,082,018	2,309,727	0.15%
	Number of impressions of Search interventions (Covid-19)	Number of clicks of Search interventions (Covid-19)	Click Through Rate of Search interventions (Covid-19)
Member States			
Austria	70,050	82	0.12%
Belgium	87,626	88	0.10%
Bulgaria	31,310	62	0.20%
Croatia	26,304	22	0.08%
Cyprus	11,099	14	0.13%
Czech Republic	63,159	61	0.10%



Denmark	31,441	29	0.09%
Estonia	12,143	25	0.21%
Finland	44,478	71	0.16%
France	718,595	547	0.08%
Germany	681,694	470	0.07%
Greece	83,031	89	0.11%
Hungary	86,179	110	0.13%
Ireland	170,381	85	0.05%
Italy	1,269,745	1,694	0.13%
Latvia	25,296	44	0.17%
Lithuania	25,417	48	0.19%
Luxembourg	6,282	12	0.19%
Malta	6,174	5	0.08%
Netherlands	133,393	102	0.08%
Poland	392,086	243	0.06%
Portugal	153,957	101	0.07%
Romania	225,975	230	0.10%
Slovakia	29,765	35	0.12%



Slovenia	15,078	20	0.13%
Spain	1,076,579	1,091	0.10%
Sweden	112,001	94	0.08%
Iceland	5481	8	0.15%
Liechtenstein	131	0	0.00%
Norway	61,334	54	0.09%
Total EU	5,589,238	5474	0.10%
Total EEA	5,656,184	5536	0.10%

	Number of impressions of Search interventions (Covid-19 Vaccine)	Number of clicks of Search interventions (Covid-19 Vaccine)	Click Through Rate of Search interventions (Covid-19 Vaccine)
Member States			
Austria	1,834	18	0.98%
Belgium	400	2	0.50%
Bulgaria	304	0	0.00%
Croatia	337	3	0.89%
Cyprus	105	2	1.90%
Czech Republic	703	6	0.85%
Denmark	315	1	0.32%



Estonia	52	0	0.00%
Finland	323	2	0.62%
France	2,824	21	0.74%
Germany	22,837	197	0.86%
Greece	680	1	0.15%
Hungary	484	3	0.62%
Ireland	1,085	3	0.28%
Italy	10,620	62	0.58%
Latvia	140	0	0.00%
Lithuania	221	1	0.45%
Luxembourg	35	1	2.86%
Malta	48	1	2.08%
Netherlands	954	5	0.52%
Poland	1,316	3	0.23%
Portugal	2,378	5	0.21%
Romania	3,206	16	0.50%
Slovakia	290	3	1.03%
Slovenia	117	0	0.00%



Spain	1,682	11	0.65%
Sweden	1,736	7	0.40%
Iceland	47	0	0.00%
Liechtenstein	5	0	0.00%
Norway	544	2	0.37%
Total EU	55,026	374	0.68%
Total EEA	55,622	376	0.68%
	Number of impressions of Search interventions (Holocaust Misinformation/Denial)	Number of clicks of Search interventions (Holocaust Misinformation/Denial)	Click Through Rate of Search interventions (Holocaust Misinformation/Denial)
Member States			
Austria	322,916	6,753	2.09%
Belgium	383,086	5,567	1.45%
Bulgaria	144,112	1,966	1.36%
Croatia	169,828	3,241	1.91%
Cyprus	60,779	580	0.95%
Czech Republic	226,864	3,612	1.59%
Denmark	198,498	2,417	1.22%
Estonia	48,151	713	1.48%
Finland	342,976	3,551	1.04%



France	1,933,962	24,219	1.25%
Germany	2,795,563	71,817	2.57%
Greece	1,189,516	6,683	0.56%
Hungary	273,033	6,559	2.40%
Ireland	278,728	2,943	1.06%
Italy	958,194	15,816	1.65%
Latvia	54,526	1,001	1.84%
Lithuania	95,089	1,199	1.26%
Luxembourg	21,381	396	1.85%
Malta	15,110	206	1.36%
Netherlands	947,560	9,468	1.00%
Poland	843,228	826	0.10%
Portugal	254,263	2,710	1.07%
Romania	437,710	7,127	1.63%
Slovakia	114,423	1,855	1.62%
Slovenia	70,478	1,413	2.00%
Spain	1,000,503	38,723	3.87%
Sweden	517,411	7,105	1.37%



Iceland	12986	267	2.06%
Liechtenstein	564	13	2.30%
Norway	263,583	3,881	1.47%
Total EU	13,697,888	228466	1.67%
Total EEA	13,975,021	232627	1.66%
	Number of impressions of Search interventions (MPox)	Number of clicks of Search interventions (MPox)	Click Through Rate of Search interventions (MPox)
Member States			
Austria	1,426	2	0.14%
Belgium	1,840	2	0.11%
Bulgaria	938	1	0.11%
Croatia	648	3	0.46%
Cyprus	122	0	0.00%
Czech Republic	916	1	0.11%
Denmark	1,096	0	0.00%
Estonia	172	0	0.00%
Finland	1,718	8	0.47%
France	6,712	6	0.09%
Germany	10,920	11	0.10%



Greece	2,676	4	0.15%
Hungary	1,674	6	0.36%
Ireland	932	6	0.64%
Italy	4,318	5	0.12%
Latvia	288	0	0.00%
Lithuania	440	0	0.00%
Luxembourg	158	0	0.00%
Malta	82	0	0.00%
Netherlands	2,918	2	0.07%
Poland	3,676	5	0.14%
Portugal	20,590	12	0.06%
Romania	4,854	8	0.16%
Slovakia	504	0	0.00%
Slovenia	228	0	0.00%
Spain	3,577	1	0.03%
Sweden	4,006	4	0.10%
Iceland	58	2	3.45%
Liechtenstein	0	0	0.00%



Norway	1,652	5	0.30%
Total EU	77,429	87	0.11%
Total EEA	79,139	94	0.12%

	Number of impressions of Search interventions (Climate change)	Number of clicks of Search interventions (Climate change)	Click Through Rate of Search interventions (Climate change)
Member States			
Austria	288,003	63	0.02%
Belgium	195,359	79	0.04%
Bulgaria	78,024	44	0.06%
Croatia	121,172	38	0.03%
Cyprus	18,949	6	0.03%
Czech Republic	118,482	45	0.04%
Denmark	178,115	39	0.02%
Estonia	37,938	14	0.04%
Finland	257,119	85	0.03%
France	531,888	238	0.04%
Germany	2,619,383	540	0.02%
Greece	190,990	118	0.06%



Hungary	202,979	95	0.05%
Ireland	284,474	49	0.02%
Italy	840,677	337	0.04%
Latvia	45,013	26	0.06%
Lithuania	85,383	51	0.06%
Luxembourg	16,132	8	0.05%
Malta	11,624	2	0.02%
Netherlands	525,099	156	0.03%
Poland	578,227	238	0.04%
Portugal	241,710	92	0.04%
Romania	305,425	161	0.05%
Slovakia	72,635	31	0.04%
Slovenia	47,068	28	0.06%
Spain	830,170	227	0.03%
Sweden	757,723	118	0.02%
Iceland	5998	7	0.12%
Liechtenstein	422	0	0.00%
Norway	317,357	66	0.02%



Total EU	9,479,761	2,928	0.03%
Total EEA	9,803,538	3,001	0.03%

	Number of impressions of Public service announcements (Covid-19)	Number of impressions of Public service announcements (Covid 19 Vaccine)	Number of impressions of Public service announcements (Holocaust Misinformation/Denial)
Member States			
Austria	48	3	36
Belgium	42	21	264
Bulgaria	17	7	16
Croatia	16	8	17
Cyprus	3	3	6
Czech Republic	30	19	36
Denmark	22	7	35
Estonia	7	0	10
Finland	41	9	57
France	252	165	2,386
Germany	397	25	384
Greece	78	16	44
Hungary	31	20	70



Ireland	34	12	46
Italy	583	115	103
Latvia	14	4	11
Lithuania	10	2	16
Luxembourg	3	1	6
Malta	5	2	2
Netherlands	96	3	109
Poland	170	15	140
Portugal	52	4	34
Romania	72	25	41
Slovakia	19	3	14
Slovenia	6	3	10
Spain	246	37	52
Sweden	68	38	77
Iceland	7	2	6
Liechtenstein	0	0	0
Norway	31	6	33
Total EU	2,362	567	4022



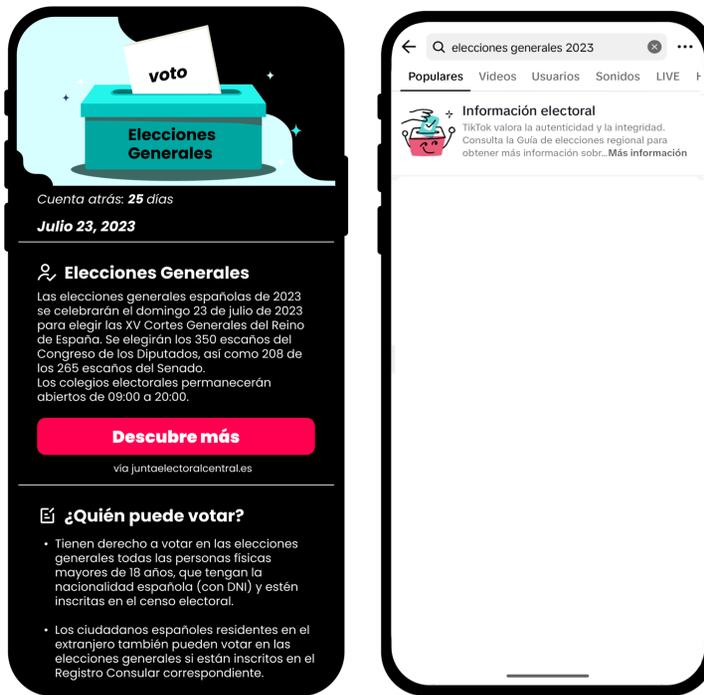
Total EEA	2,400	575	4061
	Number of impressions of Public service announcements (MPox)	Number of impressions of the safety center page on Covid-19	Number of impressions of the safety center page on election integrity
Member States			
Austria	0	2,714	277
Belgium	2	4,087	493
Bulgaria	0	5,218	517
Croatia	2	989	74
Cyprus	0	742	69
Czech Republic	0	1,838	173
Denmark	0	1,199	86
Estonia	0	372	25
Finland	1	1,463	176
France	3	33,404	2,747
Germany	5	32,705	3,360
Greece	1	4,069	380
Hungary	1	3,352	267
Ireland	10	1,983	697
Italy	4	25,371	1,650



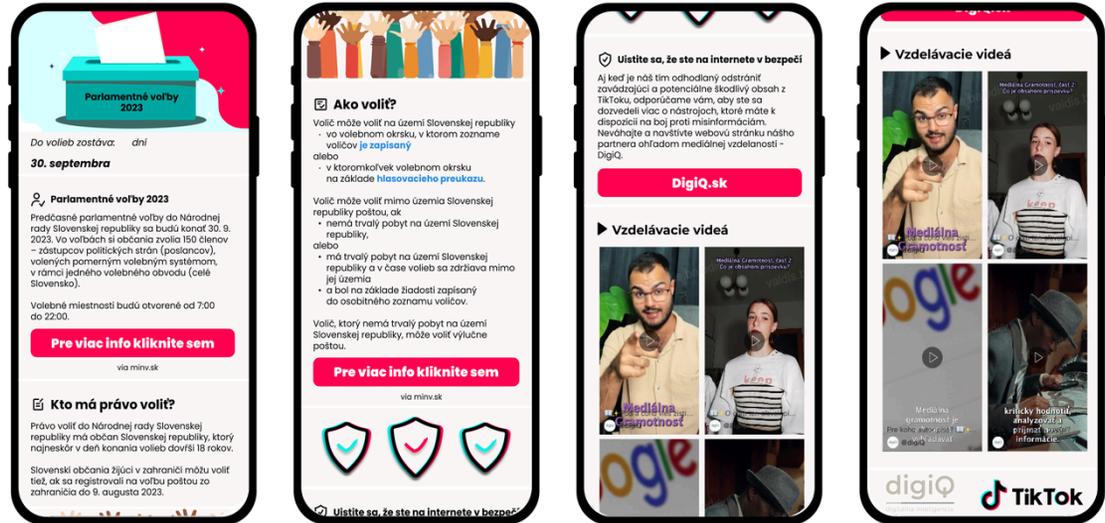
Latvia	0	825	67
Lithuania	0	794	74
Luxembourg	0	413	35
Malta	0	283	24
Netherlands	2	6,320	637
Poland	3	6,872	694
Portugal	8	3,450	193
Romania	3	13,332	744
Slovakia	0	1,015	122
Slovenia	0	469	29
Spain	2	19,631	1,456
Sweden	2	3,726	446
Iceland	0	150	11
Liechtenstein	0	12	0
Norway	1	1,689	172
Total EU	49	176636	15512
Total EEA	50	178487	15695



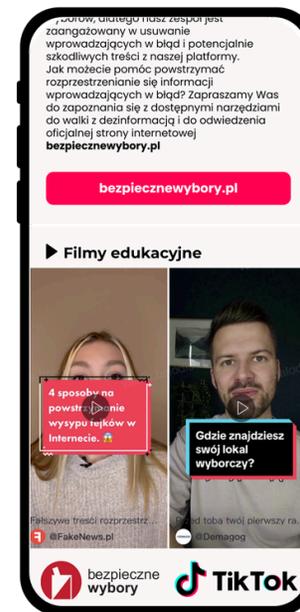
<p>Measure 17.2</p>	
<p>QRE 17.2.1</p>	<p>In order to raise awareness among our users about specific topics and empower them, we run a variety of on and off-platform media literacy campaigns. Our approach may differ depending on the topic. We localise certain campaigns (e.g., for elections) meaning we collaborate with national partners to develop an approach that best resonates with the local audience. For other campaigns such as the War in Ukraine, our emphasis is on scalability and connecting users to accurate and trusted resources.</p> <p>Below are examples of the campaigns we have most recently run in-app which have leveraged a number of the intervention tools we have outlined in our response to QRE 17.1.1 (e.g. search interventions and video notice tags).</p> <p>(I) Promoting election integrity. As well as the election integrity pages on TikTok's Safety Center and Transparency Center, which bring awareness and visibility to how we tackle election misinformation and covert influence operations on our platform, we launched media literacy campaigns in advance of several major European elections.</p> <p>2023 Spanish election (23rd July). We launched a search intervention and in-app Election Center to provide users with up-to-date information in advance of the Spanish general election. We worked with Newtral, our fact-checking partner, and Maldita, a local media literacy organisation, to produce educational videos about the electoral process and election misinformation.</p>



2023 Slovak election (30th Sept). We partnered with DigiQ to develop our media literacy strategy with the objective of educating users on how to detect misinformation and verify information they are seeing online. Official voting information and educational videos were available in our in-app Slovak Election Center, which redirected users to authoritative information on DigiQ's website.



2023 Polish election (15th Oct). We partnered with Demagog and FakeNews.pl to develop our media literacy strategy with the objective of educating users on how to detect misinformation and verify information they are seeing online. We rolled out a campaign, comprising a search intervention, video notice tag and official voting information through an In-App Polish Election Center, including educational videos, which redirected users to authoritative information.



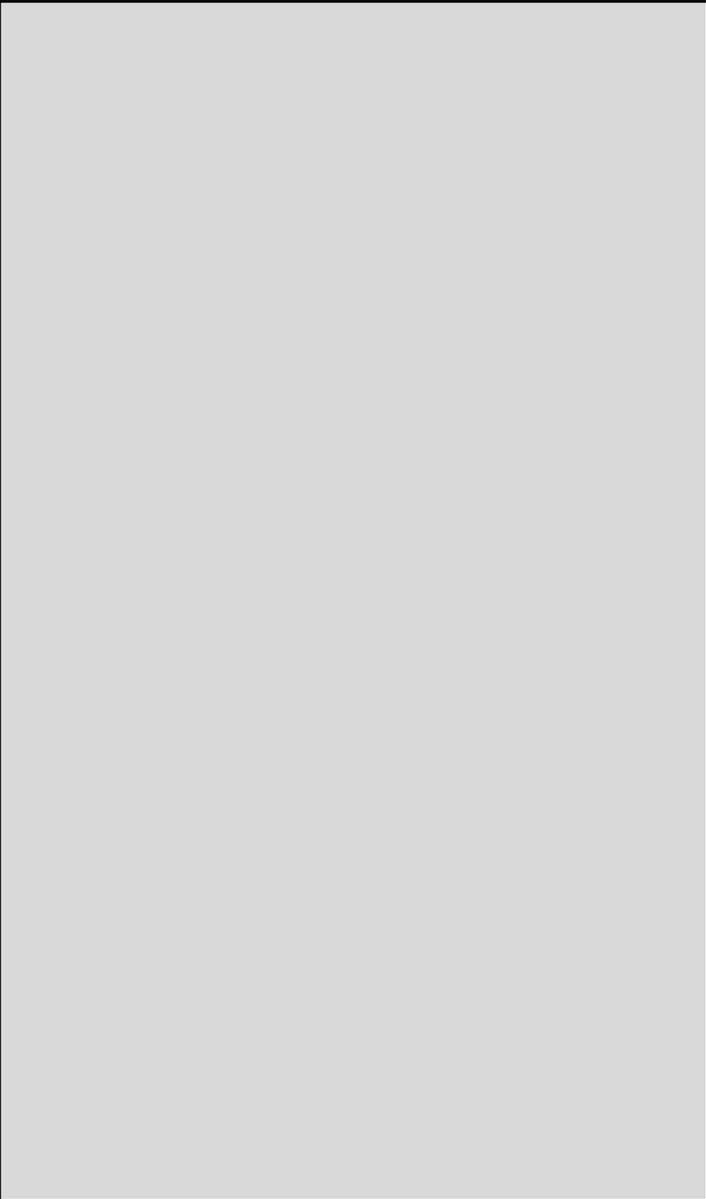
2023 Dutch election (22nd Nov). We worked with [Deutsche Presse-Agentur](#) (DPA), our fact-checking partner, and [Nieuwscheckers](#), a fact-checking initiative of the [Journalism and New Media course](#) at Leiden University to provide users with up-to-date information, including educational videos about media literacy on TikTok in advance of the Dutch parliamentary election through a search intervention and in-app Dutch Election Center. We also published a dedicated [Newsroom post](#) to highlight our efforts.



(II) Election Speaker Series. To further promote election integrity, and inform our approach to country-level EU elections, we invited suitably qualified local and regional external experts to share their insights and market expertise with our internal teams. Our recent Election Speaker Series heard presentations from our local fact-checking partners, Newtral for Spain, Demagog for Poland, DPA for Netherlands and our online safety association partner DigiQ for Slovakia.

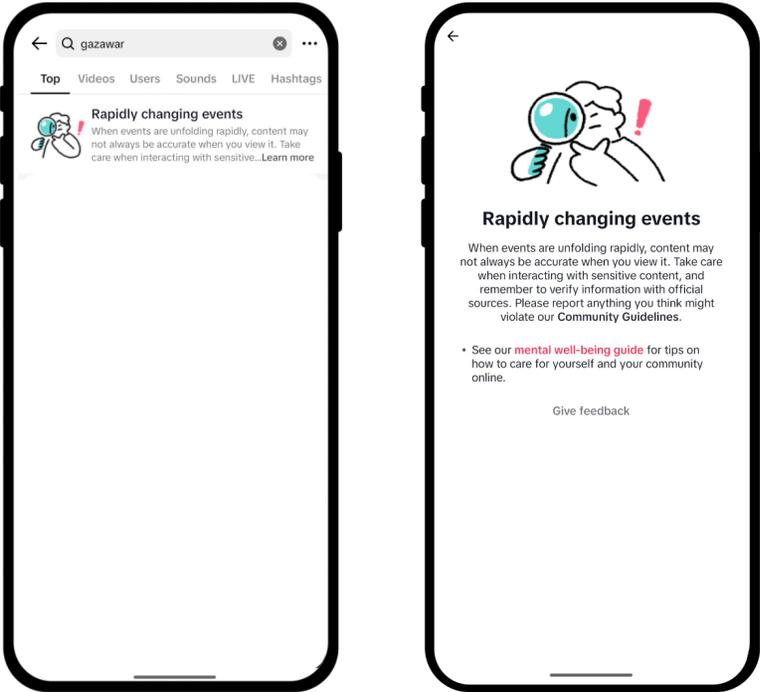
(III) Media literacy (General). We rolled out five general media literacy and critical thinking skills campaigns in Finland, Ireland, Italy, Spain and Sweden in this reporting period. See details of the campaign in [Ireland](#). We have ambitious plans to continue to develop and roll out media literacy campaigns this year in partnership with our trusted fact-checking partners and achieve localised activations in all 27 Member States by the end of 2024, with the majority being activated ahead of the European Parliamentary Elections.

(IV) Media literacy (war in Ukraine). We rolled out six new media literacy campaigns in Europe during this reporting period, in Austria, Bulgaria, Czech Republic, Croatia, Germany and Slovenia, that were specific to the war in Ukraine. This builds on the eight localised media literacy campaigns about the war in [Poland](#), Slovakia, Romania, Ukraine, Hungary, Estonia,



Latvia and Lithuania in the previous reporting period. Through these media literacy campaigns, users searching for keywords relating to the war in Ukraine on TikTok are directed to tips prepared in partnership with local media literacy bodies and our trusted fact-checking partners, to help them identify misinformation and prevent its spread on the platform.

(V) Israel-Hamas conflict. To help raise awareness and to protect our users, we have launched search interventions which are triggered when users search for non-violative terms related to this topic (e.g., Israel, Palestine). These search interventions remind users to pause and check their sources and also directs them to well-being resources.



(VI) Climate literacy.

- Our [climate change search intervention tool](#) launched in April 2023 and is available in 23 official EU languages (plus Norwegian and Icelandic for EEA users). It redirects



	<p>users looking for climate change-related content to authoritative information and encourages them to report any potential misinformation they see.</p> <ul style="list-style-type: none"> • Coinciding with COP 26 in 2021, we launched a global #ClimateAction campaign to encourage communities all over the world to join climate conversations and take action that has a positive impact on our planet. To date, the annual campaign has garnered over 2 billion video views globally. • In November 2023 we launched a new \$1M initiative to tackle climate misinformation in support of Verified for Climate. This is a joint program of the United Nations and Purpose. Verified works with a range of civil society groups, media broadcasters, activists, and companies around the world to help deliver Verified information to millions of people. The initiative will bring together a team of Verified Champions, including scientists and trusted experts from Brazil, the United Arab Emirates, Spain, and select TikTok creators to develop educational content tackling climate misinformation and disinformation while driving climate action within the TikTok community. Verified Champions is a network of climate messengers with the credibility and experience to share life and planet-saving information. 			
<p>SLI 17.2.1 - actions enforcing policies above</p>	<p>We are pleased to report metrics on the 11 media literacy and critical thinking skills campaigns that we rolled out in this reporting period:</p> <ul style="list-style-type: none"> • Six (Austria, Bulgaria, Czech Republic, Croatia, Germany and Slovenia) were specific to the war in Ukraine, including identifying misinformation and manipulated media reports. • Five (Finland, Ireland, Italy, Spain and Sweden) were focused on general media literacy and critical thinking skills. <p>A number of these campaigns launched at the end of December 2023, which means the impression numbers reported below are limited. These campaigns have continued to run into 2024, and we will provide updated figures for these campaigns in our next report.</p>			
<p>Member States</p>	<p>Total number of impressions of the H5 Page (Views generated till</p>	<p>Number of impressions of the search intervention</p>	<p>Number of clicks on the search intervention</p>	<p>Click through rate of the search intervention</p>



	December 31st,2023)			
Ireland, in partnership with The journal.ie	50,814	972,922	1,525	0.16%
Finland, in partnership with Logically Facts	3,359	31,195	155	0.50%
Sweden, in partnership with Logically Facts	10,118	71,584	180	0.25%
Spain, in partnership with Maldita	54,047	775,661	580	0.07%
Italy, in partnership with Facta	352	50,912	88	0.17%
Austria and Germany, in partnership with Correctiv	87,783	16,105,548	83,585	0.52%
Bulgaria	80	35,760	65	0.18%
Croatia	49	31,660	44	0.14%
Czech Republic	113	117,190	95	0.08%
Slovenia	24	7,640	19	0.25%
Member States	Number of Ads run for the media literacy campaign	Number of impressions of the Ads	Number of clicks on the Ads	Click through rate of the Ads
Ireland, in partnership with The journal.ie	5	12,398,400	113018	0.91%
Finland, in partnership with Logically Facts	3	4,946,201	32,696	0.66%
Sweden, in partnership with Logically Facts	3	12,456,639	117,770	0.95%



Spain, in partnership with Maldita	3	23,471,585	139,846	0.60%
Italy, in partnership with Facta	5	27,515,776	262,127	0.95%
Austria and Germany, in partnership with Correctiv	5	92,386,860	394,265	0.71%

Measure 17.3	
QRE 17.3.1	<p>As documented in the TikTok Safety Center Safety Partners page, we work with an array of industry experts, non-governmental organisations, and industry associations around the world in our commitment to building a safe platform for our community. They include media literacy bodies, to develop campaigns that educate users and redirect them to authoritative resources, and fact-checking partners. Specific examples of partnerships within the campaigns and projects set out in QRE 17.2.1 are:</p> <p>(I) Promoting election integrity. We partner with various media organisations and fact-checkers to promote election integrity on TikTok. For more detail about the input our fact-checking partners provide please refer to QRE 30.1.3.</p> <ul style="list-style-type: none"> • Polish election. When designing our overall program for the Polish election, we considered the local risks identified by key stakeholders and experts including Demagog and BezpieczneWybory.pl, initiated by the National Research Institute (NASK). We worked with our original fact-checking partner, the German Press Agency (DPA), and our newly onboarded Polish Fact-Checking Program partner, Demagog. • Dutch election. We worked with Deutsche Presse-Agentur (DPA), our fact-checking partner, and Nieuwscheckers, a fact-checking initiative of the Journalism and New Media course at Leiden University to provide users with up-to-date information, including educational videos about media literacy on TikTok in advance of the Dutch parliamentary election through a search intervention and in-app Dutch Election Center. • Election speaker series. To further promote election integrity, and inform our approach to country-level EU elections, we invited suitably qualified local and regional external experts to share their insights and market expertise with our internal teams. Our recent Election Speaker Series heard presentations from our local fact-checking partners, Newtral for Spain, Demagog for Poland, DPA for Netherlands and our online safety association partner DigiQ for Slovakia.



	<p>(II) War in Ukraine. We launched our media literacy campaigns about the war in Ukraine with our media literacy partners Correctiv in Austria and Germany and Lead Stories in Bulgaria, Czech Republic, Croatia, and Slovenia.</p> <p>(III) Covid-19. In relation to Covid-19 misinformation, we have continued our partnerships with: (i) the WHO Tech Taskforce; and (ii) our European fact-checkers including AFP, Facta, Logically, Lead Stories, Newtral, Science Feedback, Teyit, DPA, Reuters, and Demagog (who we have recently onboarded in Europe). Our partners provide us with information about Covid-19 trends including new variants, vaccine side effects on adults and children, and information about new treatments (such as antivirals). This information helps us improve our in-app intervention tools.</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.	
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].	<ul style="list-style-type: none"> Continued to scale-up our fact-checking program, expanding to two new EU countries (Croatia and Portugal). We will be expanding our misinformation moderation teams' coverage accordingly. Onboarded two new local fact-checking partners Demagog (Poland) and Poligrafo (Portugal). Continued our detection and labelling of designated state-affiliated media in Europe and Asia and expanded the availability of state-controlled media labels to Sub-Saharan Africa, further increasing transparency for EU users.



	<ul style="list-style-type: none"> • Participated in the data access pilot with EDMO, trialling the process for sharing data with vetted researchers as designated under the DSA. • Actively participating in the EDMO working group for the creation of the Independent Intermediary Body (IIB) to support research on digital platforms. • Invested in training and development for our Trust and Safety team, including regular internal sessions dedicated to knowledge sharing and discussion about relevant issues and trends and external events to share expertise and support their continued professional learning. For example, members of our Trust and Safety team (including leaders of our fact-checking program) attended the Global Fact 10 Global Fact-Checking Conference hosted by the International Fact-Checking Network in June 2023 and hosted a panel discussion on our approach to countering harmful misinformation. • Engaged with external experts when updating or launching new policies or features on our platform, including on harmful misinformation, elections, and our state-affiliated media policy and new AI-generated content label.
<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]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> • Ensuring fact-checking coverage by a combination of permanent and temporary partnerships covering at least one official language of each of the European Member States ahead of the EU Elections. We will be expanding our misinformation moderation teams' coverage accordingly. • Continuing to improve the accuracy of, and overall coverage provided by, our machine learning detection models. • Building on our efforts to raise users' awareness about the credibility of content and to encourage people to reconsider sharing unverified content by expanding the application of our unverified content label to high risk and crisis events.



	<ul style="list-style-type: none"> • Continuing to invest in training and development for our Trust and Safety team with the help of our fact-checking partners and external experts in this field, including by continuing the Election Speaker Series in advance of major EU elections. • Continuing to work with our fact-checking and media literacy partners to develop our media literacy strategy educating users on how to detect misinformation and verify information they are seeing online. • Continuing to participate in, and co-chair, the working group on Elections.
<p>Measure 18.1</p>	
<p>QRE 18.1.1</p>	<p>TikTok takes a multi-faceted approach to tackling the spread of harmful misinformation, regardless of intent. This includes our policies, products, practices and external partnerships with fact-checkers, media literacy bodies, and researchers.</p> <p>(I) Removal of violating content or accounts. To reduce potential harm, we aim to remove content or accounts that violate our CGs including our I&A policies before they are viewed or shared by other people. We detect and take action on this content by using a combination of automation and human moderation.</p> <p>a) Automated Review. We place considerable emphasis on proactive detection to remove violative content. Content that is uploaded to the platform is typically first reviewed by our automated moderation technology, which looks at a variety of signals across content, including keywords, images, titles, descriptions, and audio, to identify violating content. We work with various external experts, like our fact-checking partners, to inform our keyword lists. If our automated moderation technology identifies content that is a potential violation, it will either be automatically removed from the platform or flagged for further review by our human moderation teams. In line with our safeguards to help ensure accurate decisions are made, automated removal is applied when violations are the most clear-cut. We also carry out targeted sweeps of certain types of violative content including harmful misinformation, where we</p>



have identified specific risks or where our fact-checking partners or other experts have alerted us to specific risks.

- b) **Human Moderation.** While some misinformation can be enforced through technology alone—for example, repetitions of previously debunked content—misinformation evolves quickly and is highly nuanced. This is why we have misinformation moderators with enhanced training and access to tools such as our global repository of previously fact-checked claims from the IFCN-accredited fact-checking partners, who help assess the accuracy of content. We also have teams on the ground who partner with experts to prioritise local context and nuance. We may also issue guidance to our moderation teams to help them more easily spot and take swift action on violating content. Human moderation will also occur if a video gains popularity or has been reported. Community members can report violations in-app and on our website. Our fact-checking partners and other stakeholders can also report potential violating content to us directly.

(II) Safety in our recommendations. In addition to removing content that clearly violates our CGs, we have a number of safeguards in place to ensure the For You feed (as the primary access point for discovering original and entertaining content on the platform) has safety built-in.

- a. For content that does not violate our CGs but may negatively impact the authenticity of the platform, we reduce its prominence on the For You feed and / or label it. The types of misinformation we may make For You feed ineligible are now made even clearer to users [here](#); general conspiracy theories, unverified information related to an emergency or unfolding event and potential high-harm misinformation that is undergoing a fact-check. We also label accounts and content of state-affiliated media entities to empower users to consider the sources of information. Our moderators take additional precautions to review videos as they rise in popularity to reduce the likelihood of content that may not be appropriate entering our recommended system.
- b. Providing access to authoritative information is an important part of our overall strategy to counter misinformation. There are a number of ways in which we do this, including launching information centers with informative



	<p>resources from authoritative third-parties in response to global or local events, adding public service announcements on hashtag or search pages, or labelling content related to a certain topic to prompt our community to seek out authoritative information.</p> <p>(III) Safety by Design. Within our Trust and Safety Product and Policy teams, we have subject matter experts dedicated to integrity and authenticity. When we develop a new feature or policy, these teams work closely with external partners to ensure we are building safety into TikTok by design and reflecting industry best practice. For example:</p> <ul style="list-style-type: none"> • We collaborated with Irrational Labs to develop and implement specialised prompts to help users consider before sharing unverified content (as outlined in QRE 21.3.1), • Yad Vashem created an enrichment program on the Holocaust for our Trust and Safety team. The five week program aimed to give our team a deeper understanding about the Holocaust, its lessons and misinformation related to antisemitism and hatred. • We work with local/regional experts through our Election Speaker Series to ensure their insights and expertise informs our internal teams in the lead up to EU elections (as outlined in QRE 17.3.1).
<p>QRE 18.1.2</p>	<p>The For You feed is the interface users first see when they open TikTok. It's central to the TikTok experience and where most of our users spend their time exploring the platform. The system recommends content by ranking videos based on a combination of factors including:</p> <ul style="list-style-type: none"> • user selections (i.e. interest categories indicated in the registration process or selecting “not interested” on content); • user interactions (i.e. videos users like/share, watch in full or skip accounts users follow, accounts that follow users, comments users post and content they create); • video information (i.e. captions/sounds and hashtags used, number of video views, and the country in which the video was published.); and



	<ul style="list-style-type: none"> • device and account settings (i.e. language preferences, country settings, time zone and day, and device types). <p>All these factors are weighted based on their value to a user and the recommendation system then ranks them to determine the likelihood of a user’s interest in a particular category of content. The weighting of a factor can change dynamically. We share more information about our recommender system in our Transparency Center and below in our response to QRE 19.1.1.</p>
<p>QRE 18.1.3</p>	<p>We take action to prevent and mitigate the spread of inaccurate, misleading, or false misinformation that may cause significant harm to individuals or the public at large. We do this by removing content and accounts that violate our rules, investing in media literacy and connecting our community to authoritative information, and partnering with external experts. Our I&A policies make clear that we do not allow activities that may undermine the integrity of our platform or the authenticity of our users. We remove content or accounts that involve misleading information that causes significant harm or, in certain circumstances, reduce the prominence of content. The types of misinformation we may make ineligible For You feed are set out in our Community Guidelines.</p> <ul style="list-style-type: none"> • Misinformation <ul style="list-style-type: none"> ○ General conspiracy theories that are unfounded and claim that certain events or situations are carried out by covert or powerful groups, such as “the government” or a “secret society”. ○ Unverified information related to an emergency or unfolding event where the details are still emerging. ○ Potential high-harm misinformation while it is undergoing a fact-checking review. • Civic and Election Integrity <ul style="list-style-type: none"> ○ Unverified claims about the outcome of an election that is still unfolding and may be false or misleading. <p>To enforce our CGs at scale, we use a combination of automated review and human moderation. While some misinformation can be enforced through technology alone—for example, repetitions of previously debunked content—misinformation evolves quickly and is highly nuanced. Assessing harmful misinformation requires additional context and</p>



	<p>assessment by our misinformation moderators who have enhanced training, expertise and tools to identify such content, including our global repository of previously fact-checked claims from the IFCN-accredited fact-checking partners and direct access to our fact-checking partners where appropriate.</p> <p>Our network of independent fact-checking partners do not moderate content directly on TikTok, but assess whether a claim is true, false, or unsubstantiated so that our moderators can take action based on our Community Guidelines. We incorporate fact-checker input into our broader content moderation efforts through:</p> <ul style="list-style-type: none"> • Proactive insight reports that flag new and evolving claims they're seeing across the internet. This helps us detect harmful misinformation and anticipate misinformation trends on our platform. • A repository of previously fact-checked claims to help misinformation moderators make swift and accurate decisions. <p>Working with our network of independent fact-checking organisations enables TikTok to identify and take action on misinformation and connect our community to authoritative information around important events. This is an important part of our overall strategy to counter misinformation. There are a number of ways in which we do this, including launching information centers with resources from authoritative third-parties in response to global or local events, adding public service announcements (PSAs) on hashtags or search pages, or labelling content related to a certain topic to prompt our community to seek out authoritative information.</p> <p>We are also committed to civic and election integrity and mitigating the spread of false or misleading content about an electoral or civic process. We work with national electoral commissions, media literacy bodies and civil society organizations to ensure we are providing our community with accurate up-to-date information about an election through our in-app election information centers, election guides, search interventions, content labels and hashtag PSAs.</p>
<p>SLI 18.1.1 - actions proving effectiveness of measures and policies</p>	<p>Methodology of data measurement:</p> <p>The share cancel rate (%) following the unverified content label share warning pop-up indicates the percentage of users who do not share a video after seeing the label pop up. This metric is based on the approximate location of the users that engaged with these tools.</p>



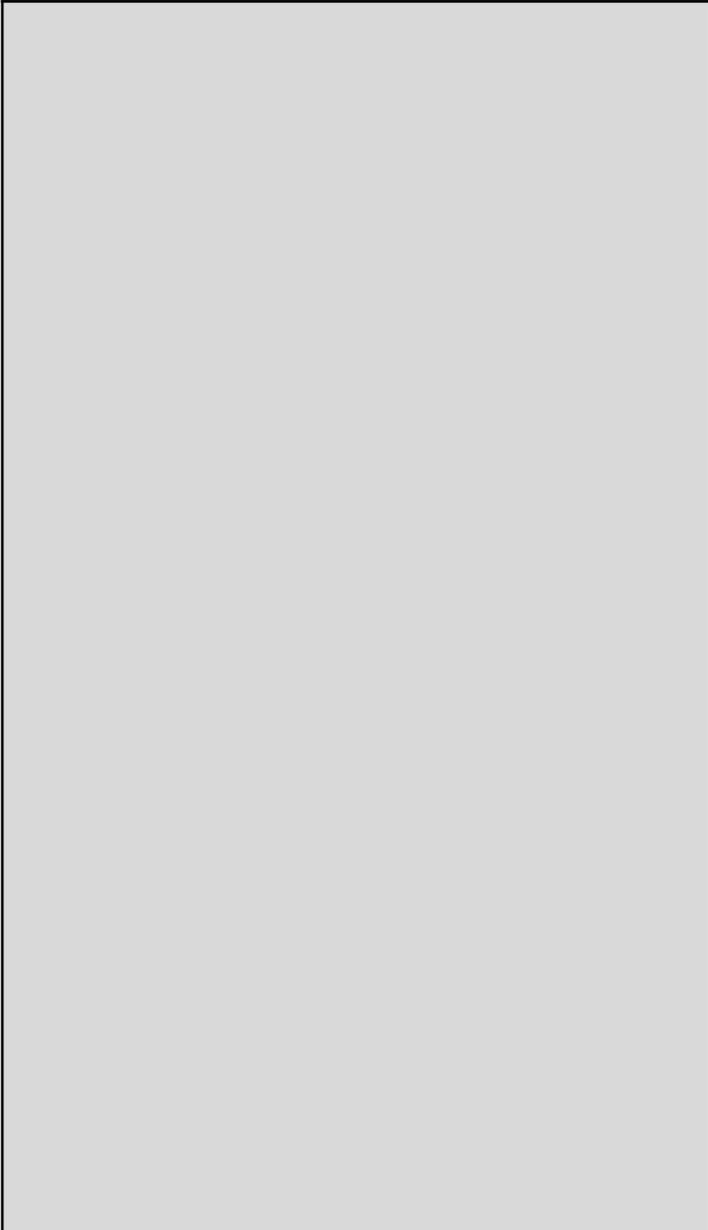
				Other relevant metrics
List actions per member states and languages (see example table above)				Share cancel rate (%) following the unverified content label share warning pop-up (users who do not share the video after seeing the pop up)
Member States				
Austria				32.08%
Belgium				22.45%
Bulgaria				27.31%
Croatia				27.56%
Cyprus				27.93%
Czech Republic				28.32%
Denmark				22.83%
Estonia				39.34%
Finland				24.05%



France				24.85%
Germany				34.57%
Greece				28.30%
Hungary				27.18%
Ireland				25.86%
Italy				26.83%
Latvia				30.23%
Lithuania				28.32%
Luxembourg				28.83%
Malta				28.17%
Netherlands				23.46%
Poland				29.19%
Portugal				28.48%
Romania				27.30%
Slovakia				20.61%
Slovenia				20.44%
Spain				28.53%



Sweden				26.00%
Iceland				28.57%
Liechtenstein				0.00%
Norway				25.88%
Total EU				28.93%
Total EEA				28.84%
Measure 18.2				
QRE 18.2.1	<p>We take action against misinformation that causes significant harm to individuals, our community, or the larger public regardless of intent. We do this by removing content and accounts that violate our rules, by investing in media literacy and connecting our community to authoritative information, and by partnering with experts.</p> <p>Our Terms of Service and I&A policies under our CGs are the first line of defence in combating harmful misinformation and (as outlined in more detail in QRE 14.1.1) deceptive behaviours on our platform. These rules make clear to our users what content we remove or make ineligible for the For You feed when they pose a risk of harm to our users and our community.</p> <p>Specifically, our policies do not allow:</p> <ul style="list-style-type: none"> • Misinformation that poses a risk to public safety or may induce panic about a crisis event or emergency. • Medical misinformation, such as misleading statements about vaccines, inaccurate medical advice that discourages people from getting appropriate medical care for a life-threatening disease, and other misinformation that poses a risk to public health. • Climate change misinformation that undermines well established scientific consensus, such as denying the existence of climate change or the factors that contribute to it. • Dangerous conspiracy theories that are violent or hateful. • Specific conspiracy theories that name and attack individual people. 			



- Material that has been edited, spliced, or combined (such as video and audio) in a way that may mislead a person about real-world events.
- Election misinformation.

We have made even clearer to our users [here](#) that the following content is ineligible for the For You feed:

- General conspiracy theories that are unfounded and claim that certain events or situations are carried out by covert or powerful groups.
- Unverified information related to an emergency or unfolding event where the details are still emerging.
- Potential high-harm misinformation while it is undergoing a fact-checking review.

As outlined in the QRE 14, we also remove accounts that seek to mislead people or use TikTok to deceptively sway public opinion. These activities range from inauthentic or fake account creation, to more sophisticated efforts to undermine public trust.

We have policy experts within our Trust and Safety team dedicated to the topic of integrity and authenticity. They continually keep these policies under review and collaborate with external partners and experts to understand whether updates or new policies are required and ensure they are informed by a diversity of perspectives, expertise, and lived experiences. In particular, our Safety Advisory Council for Europe, which brings together independent leaders from academia and civil society, represent a diverse array of backgrounds and perspectives, and are made up of experts in free expression, misinformation and other safety topics. They work collaboratively with us to inform and strengthen our policies, product features, and safety processes.

Enforcing our policies. We remove content – including video, audio, livestream, images, comments, links, or other text – that violates our I&A policies. Individuals are notified of our decisions and can appeal them if they believe no violation has occurred. We also make clear in our CGs that we will temporarily or permanently ban accounts and/or users that are involved in serious or repeated violations, including violations of our I&A policies.

We enforce our CGs policies, including our I&A policies, through a mix of technology and human moderation. To do this effectively at scale, we continue to invest in our automated review process as well as in people and training. At TikTok we place a considerable emphasis on proactive content moderation. This means our teams work to detect and remove harmful material before it is reported to us.



	<p>However, misinformation is different from other content issues. Context and fact-checking are critical to consistently and accurately enforcing our misinformation policies. So while we use machine learning models to help detect potential misinformation, ultimately our approach today is having our moderation team assess, confirm, and remove misinformation violations. We have misinformation moderators who have enhanced training, expertise, and tools to take action on harmful misinformation. This includes a repository of previously fact-checked claims to help misinformation moderators make swift and accurate decisions and direct access to our fact-checking partners who help assess the accuracy of new content.</p> <p>We strive to maintain a balance between freedom of expression and protecting our users and the wider public from harmful content. Our approach to combating harmful misinformation, as stated in our CGs, is to remove content that is both false and can cause harm to individuals or the wider public. This does not include simply inaccurate information which does not pose a risk of harm. Additionally, in cases where fact-checks are inconclusive, especially during emergency or unfolding events, content may not be removed and may instead become ineligible for recommendation in the For You feed and labelled with the “unverified content” label to limit the spread of potentially misleading information.</p> <p>We are pleased to include in this report the number of videos made ineligible for the For You feed under the relevant I&A policies (general conspiracy theories and unverified information related to an emergency or unfolding event) as explained to users here.</p> <p>Note that in relation to the metrics we have shared at SLI 18.2.1 below, of all the views that occurred in H2 2023, approximately 2 in 10,000 views occurred on content identified and removed for violating our policies around harmful misinformation.</p>		
<p>SLI 18.2.1 - actions taken in response to policy violations</p>	<p>Methodology of data measurement:</p> <p>We have based the following numbers on the country in which the video was posted: videos removed because of violations of our Misinformation and Civic and Election Integrity policies.</p> <p>The number of views of videos removed because of violation of each of these policies is based on the approximate location of the user.</p>		
<p>Total no of violations</p>	<p>Metric 1: indicating the</p>	<p>Total no of violations</p>	<p>Metric 1: indicating the impact of the action taken</p>



		impact of the action taken		
List actions per member states and languages (see example table above)	Number of videos removed because of violation of misinformation policy	Number of views of videos removed because of violation of misinformation policy	Number of videos made ineligible for the For You feed under the relevant I&A policies (general conspiracy theories and unverified information related to an emergency or unfolding event)	
Member States				
Austria	2,601	8,678,936	578	
Belgium	7,481	23,723,382	12	
Bulgaria	1,629	5,003,945	153	
Croatia	273	1,485,791	24	
Cyprus	431	1,362,234	2	
Czech Republic	2,408	5,403,481	192	
Denmark	2,270	6,652,804	93	
Estonia	92	429,270	28	
Finland	1,028	3,824,592	103	
France	74,537	236,030,201	23,834	



Germany	30,460	311,755,394	13,070
Greece	7,106	13,464,011	594
Hungary	3,100	16,813,813	191
Ireland	3,388	1,797,132	20
Italy	55,954	67,828,576	6,252
Latvia	265	63,444	0
Lithuania	256	2,475,932	5
Luxembourg	169	5,606,943	0
Malta	102	13,728	7
Netherlands	6,663	28,520,678	2,506
Poland	11,955	81,982,794	3,997
Portugal	1,804	315,508,924	162
Romania	11,671	44,197,617	2,774
Slovakia	442	3,723,359	69
Slovenia	163	408,097	14
Spain	25,053	139,908,123	25,272
Sweden	5,099	11,952,149	3,007



Iceland	50	30086	5
Liechtenstein	0	0	0
Norway	3,794	17,867,884	167
Total EU	256400	1338615350	82959
Total EEA	260244	1356513320	83131
List actions per member states and languages (see example table above)	Number of videos removed because of violation of Civic and Election Integrity policy	Number of views of videos removed because of violation of Civic and Election Integrity policy	
Member States			
Austria	233	38,060	
Belgium	213	6,616	
Bulgaria	188	427	
Croatia	24	0	
Cyprus	143	593	
Czech Republic	1,648	7,661	
Denmark	133	11,708	
Estonia	26	5,677	
Finland	1,104	33,054	
France	1,225	13,838	



Germany	744	294,536
Greece	651	0
Hungary	233	17,405
Ireland	123	8,000
Italy	2,571	54,254
Latvia	53	9,246
Lithuania	37	2,703
Luxembourg	11	299
Malta	12	0
Netherlands	912	5,762
Poland	874	3,574,124
Portugal	357	12,928
Romania	584	3,880
Slovakia	71	118,389
Slovenia	5	0
Spain	1,411	1,550
Sweden	230	21,674
Iceland	0	0
Liechtenstein	0	0
Norway	189	22,380



Total EU	13816	4242384
Total EEA	14005	4264764
Measure 18.3		
QRE 18.3.1	<p>We regularly consult with third party experts and researchers in relation to the development of policies and features which are designed to reduce the spread of disinformation. For example, during this report period, we engaged with experts globally on our Election Misinformation policies, which will help inform future updates of our I&A policies.</p> <p>We are proud of our close work with behavioural psychologists, Irrational Labs, which led to the development of the following warning and labelling features (more detail at QRE 21.3.1):</p> <ul style="list-style-type: none"> • specialised prompts for unverified content, which alert viewers to unverified content identified during an emergency or unfolding event; and • our state-controlled media label, which brings transparency to our community in relation to state affiliated media entities and raises awareness among users to encourage users to consider the reliability of the source. <p>We continue to explore ways in which we can leverage consultations carried out with researchers from the Massachusetts Institute of Technology (US) and the University of Regina (Canada) about the design of tools which would facilitate engagement with users who have interacted with harmful misinformation on our platform (more detail at QRE 21.2.1).</p> <p>We are proud to be the first signatory to the Partnership on AI's (PAI) Responsible Practices for Synthetic Media. We contributed to developing this code of industry best practices for AI transparency and responsible innovation, balancing creative expression with the risks of emerging AI technology.</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.



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].	<ul style="list-style-type: none"> • Improved user transparency of the way in which our recommender systems operate. See our updated Help Center article here and Transparency Center page. • Rolled-out a new feature that enables users to refresh their For You feed if their recommendations no longer feel relevant. • In August 2023, in the context of our obligations under the DSA (Article 38), introduced non-personalized feeds on our platform, which provide users with an alternative to recommender systems which are based on profiling. See here.
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?	<ul style="list-style-type: none"> • Continuing to explore ways in which we increase transparency for users around our recommender systems, including through additional information in our Help Center page.
Measure 19.1	
QRE 19.1.1	<p>The For You feed is the interface users first see when they open TikTok. It's central to the TikTok experience and where most of our users spend their time exploring the platform.</p> <p>We make clear to users in our Terms of Service and CGs (and also provide more context in our Help Center article and Transparency Center page) that each account holder's For You feed is based on a personalised recommendation system. The For You feed is curated to each user. Safety is built into our recommendations. As well as removing harmful misinformation content</p>



that violates our CGs, we take steps to avoid recommending certain categories of content that may not be appropriate for a broad audience including general conspiracy theories and unverified information related to an emergency or unfolding event. We may also make some of this content harder to find in search.

Main parameters. The system recommends content by ranking videos based on a combination of factors including:

- user selections (i.e. interest categories indicated in the registration process or selecting “not interested” on content);
- user interactions (i.e. videos users like/share, watch in full or skip accounts users follow, accounts that follow users, comments users post and content they create);
- video information (i.e. captions/sounds and hashtags used, number of video views, and the country in which the video was published.); and
- device and account settings (i.e. language preferences, country settings, time zone and day, and device types).

All these factors are weighted based on their value to a user and the recommendation system then ranks them to determine the likelihood of a user’s interest in a particular category of content. The weighting of a factor can change dynamically. If a user watches a longer video from beginning to end, this would be considered a strong indicator of interest and receive a greater weight than a weak indicator such as device and account settings because users don’t actively express these preferences. If a viewer never finishes watching any videos, but watches a lot of videos posted by creators in the same region, then that region may have a relatively stronger weight compared to other factors for that viewer. These predictions are also influenced by the interactions of other people on TikTok who appear to have similar interests. For example, if a user likes videos 1, 2, and 3 and a second user likes videos 1, 2, 3, 4 and 5, the recommendation system may predict that the first user will also like videos 4 and 5.

Building on our existing recommender system transparency we introduced the “Why this video” feature, which allows users to see with any particular video that appears in their For You feed factors that influenced why it appeared in their feed. This feature provides added transparency in relation to how our ranking system works and empowers our users to better understand why a particular video has been recommended to them. The feature essentially explains to users how past interactions on the platform have impacted the video they have been recommended. For further information, see our [newsroom post](#).



	<p>User preferences. Together with the safeguards we build into our platform by design, we also empower our users to customise their experience to their preferences and comfort.</p> <ul style="list-style-type: none"> • Users can click on any video and select “not interested” to automatically skip future videos from that same creator or using the same audio. • Users are able to automatically filter out videos with specific words or hashtags associated with content that they don't want to see from their For You or Following feeds (see here). • Users can enable “Restricted Mode” within their account settings in order to limit the appearance of content that may not be appropriate for all audiences. • As part of our efforts to meet DSA requirements, we are giving our European community another way to discover content on TikTok. They will be able to turn off personalisation so that their For You and LIVE feeds will instead show the most popular videos in their regions and internationally, rather than recommending content to them based on their personal interests (see here). • Users are able to refresh their For You feed if their recommendations no longer feel relevant. When the feed is refreshed, users view content on their For You feed as if they have just signed up for TikTok. Our recommendation system will then begin to surface more content based on new interactions. <p>We overhauled the design of our Creator Portal to make it more colourful and visually accessible. We created a series of informative videos specifically on the For You feed and our recommendation system. Users can also browse through the top questions and answers on our recommendation systems.</p>		
Measure 19.2			
SLI 19.2.1 – user settings	<p>Methodology of data measurement:</p> <p>The number of users who have filtered hashtags or a keyword to set preferences for For You feed, the number of times a user clicks “not interested” in relation to the For You feed, and the number of times users clicked on the For You Feed Refresh are all based on the approximate location of the users that engaged with these tools.</p>		
	No of times users actively	No of times users actively	



	engaged with these settings	engaged with these settings		
List actions per member states and languages (see example table above)	Number of users that filtered hashtags or words	Number of users that clicked on "not interested"	Number of times users clicked on the For You Feed Refresh	
Member States				
Austria	35,181	981,007	69,113	
Belgium	45,616	1,451,985	81,180	
Bulgaria	22,413	736,360	32,589	
Croatia	14,515	553,206	30,334	
Cyprus	4,267	171,423	9,684	
Czech Republic	30,241	856,942	25,071	
Denmark	24,246	620,907	23,538	
Estonia	8,236	157,947	11,657	
Finland	27,198	667,418	46,329	
France	216,231	8,658,802	407,075	
Germany	339,147	8,865,528	709,866	
Greece	38,109	1,479,737	60,599	
Hungary	33,748	1,136,110	32,479	
Ireland	37,794	871,246	49,229	
Italy	190,260	7,119,599	290,307	



Latvia	10,480	268,998	19,685	
Lithuania	14,524	321,471	23,659	
Luxembourg	3,134	72,819	5,002	
Malta	1,981	79,230	4,634	
Netherlands	91,308	2,287,407	128,235	
Poland	143,598	3,624,574	147,994	
Portugal	41,520	1,226,753	56,385	
Romania	61,637	2,764,087	192,695	
Slovakia	12,962	353,648	13,295	
Slovenia	6,741	173,240	9,953	
Spain	189,823	7,162,152	355,917	
Sweden	56,620	1,456,780	91,945	
Iceland	3378	63197	3498	
Liechtenstein	91	2346	144	
Norway	34,036	762,175	34,880	
Total EU	1,701,530	54,119,376	2,928,449	
Total EEA	1,739,035	54,947,094	2,966,971	

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.

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].	TikTok did not subscribe to this commitment. TikTok considers that it would be imprudent to commit to this measure at a time when the underlying technology remains unproven and the standards to be complied with are not yet finalised.
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?	N/A
Measure 20.1	
QRE 20.1.1	Not committed. TikTok considers that it would be imprudent to commit to this measure at a time when the underlying technology remains unproven and the standards to be complied with are not yet finalised. Once the relevant technology is proven and the standards are agreed and identifiable, TikTok will assess whether such an approach would be beneficial, taking into account existing measures in place.
Measure 20.2	



QRE 20.2.1	Not committed. Similarly to Measure 20.1, TikTok considers that it would be imprudent to commit to this measure at this time. TikTok is, however, open to reassessing in the future whether such an approach would be beneficial.
-------------------	--

V. Empowering Users	
Commitment 21	
<p>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.</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].	<ul style="list-style-type: none"> ● Continued to scale-up our fact-checking program, expanding to two new EU countries (Croatia and Portugal). We will be expanding our misinformation moderation teams' coverage accordingly. ● Onboarded two new local fact-checking partners Demagog (Poland) and Poligrafo (Portugal). ● Continued our detection and labelling of designated state-affiliated media in Europe and Asia and expanded the availability of state-controlled media labels to Sub-Saharan Africa, further increasing transparency for EU users. ● In keeping with our Synthetic and Manipulated Media Policy: <ul style="list-style-type: none"> ○ Launched a new AI-generated label for creators to disclose content that is completely AI-generated or significantly edited by AI.



	<ul style="list-style-type: none"> ○ Began testing automated AI-generated labels that we plan to apply automatically to content that we detect was edited or created with AI. ○ Introduced more clarity around AI-powered TikTok products by renaming TikTok AI effects to explicitly include "AI" in their name and corresponding effects label, and updated our guidelines for Effect House creators to do the same. ● Advanced our commitment to sustainability and climate literacy at COP28 by launching a new \$1M initiative to tackle climate misinformation in support of Verified for Climate, a joint program of the United Nations and Purpose. Verified works with a range of civil society groups, media broadcasters, activists, and companies around the world to help deliver Verified information to millions of people. ● To raise awareness and advocacy around sustainability and climate action, TikTok continued a global #ClimateAction campaign coinciding with the COP28 UN Climate Change Conference to encourage communities all over the world to join climate conversations and take action that has a positive impact on our planet. #ClimateAction has now garnered over 2 billion video views globally since the launch of the campaign at COP26.
<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]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> ● Following consultations with researchers, exploring and considering how we engage with users who have interacted with harmful misinformation on our platform and direct them to authoritative information. ● Building on our efforts to raise users' awareness about the credibility of content and to encourage people to reconsider sharing unverified content by expanding the application of our unverified content label to high risk and crisis events. ● Continuing to enhance our AI generated content detection capabilities by:



	<ul style="list-style-type: none"> ○ Testing automated AI-generated content labels that we plan to apply automatically to content that we detect was edited or created with AI. ○ Working with industry through content provenance partnerships. ● Ensuring fact-checking coverage by a combination of permanent and temporary partnerships covering at least one official language of each of the European Member States ahead of the EU Elections. We will be expanding our misinformation moderation teams' coverage accordingly.
<p>Measure 21.1</p>	
<p>QRE 21.1.1</p>	<p>We currently have 11 IFCN accredited fact checking organisations providing coverage in Europe, in 18 of the official European languages. Our response to QRE 30.1.2 sets out the specific organisations we partner with.</p> <p>We ensure that our users benefit from the context and insights provided by the fact checking organisations we partner with in the following ways:</p> <ul style="list-style-type: none"> ● Enforcement of misinformation policies. Our fact-checking partners play a critical role in helping us enforce our misinformation policies, which aim to promote a trustworthy and authentic experience for our users. We consider context and fact-checking to be key to consistently and accurately enforcing these policies, so, while we use machine learning models to help detect potential misinformation, we have our misinformation moderators assess, confirm, and take action on harmful misinformation. As part of this process, our moderators can access a repository of previously fact-checked claims and they are able to provide content to our expert fact checking partners for further evaluation. Where fact-checkers advise that content is false, our moderators take measures to assess and remove it from our platform. Our response to QRE 31.1.1 provides further insight into the way in which fact-checkers are involved in this process. ● Unverified content labelling. As mentioned above, we partner with fact checkers to assess the accuracy of content. Sometimes, our fact-checkers determine that content is not able to be confirmed or checks are inconclusive (especially during unfolding events). Where our fact-checkers provide us with an inconclusive/ unconfirmed determination, we use our unverified content label to inform viewers via a banner that a video contains



	<p>unverified content, in an effort to raise user awareness about content credibility. In these circumstances, the content creator is also notified that their video was flagged as unsubstantiated content and the video will become ineligible for recommendation in the For You feed.</p> <ul style="list-style-type: none"> ● In-app tools related to specific topics: <ul style="list-style-type: none"> ○ Covid-19. We partnered with a number of fact checkers throughout the EU in order to prevent the spread of harmful misinformation related to Covid-19 on our platform, including AFP, Facta, Logically, Lead Stories, Newtral, Science Feedback, Teyit and DPA. ○ Election integrity. We have launched campaigns in advance of several major elections aimed at educating the public about the voting process which encourage users to fact-check information with our fact-checking partners. For example, the election integrity campaign we rolled out in advance of the Dutch parliamentary election included a search intervention and setting up an in-app Election Center. We worked with Deutsche Presse-Agentur (DPA), our fact-checking partner, and Nieuwscheckers, a fact-checking initiative of the Journalism and New Media course at Leiden University, to provide users with up-to-date information, including educational videos about media literacy on TikTok. We also published a dedicated Newsroom post to highlight our efforts. ○ Climate Change. We launched a search intervention which redirects users seeking out climate change-related content to authoritative information. We worked with the UN to provide the authoritative information (see our newsroom post here). ● User awareness of our fact-checking partnerships and labels. We have published blog posts (available in more than 25 languages) and created a page on our Safety Center to raise users' awareness of our fact-checking program and labels and to support the work of our fact-checking partners.
<p>SLI 21.1.1 - actions taken under measure 21.1</p>	<p>Methodology of data measurement:</p> <p>The share of removals under our harmful misinformation policy, share of proactive removals, share of removals before any views and share of the removals within 24h are relative to the total removals of each policy.</p>



	The share cancel rate (%) following the unverified content label share warning pop-up indicates the percentage of users who do not share a video after seeing the label pop up. This metric is based on the approximate location of the users that engaged with these tools.				
	Reach of labels/ fact-checkers and other authoritative sources	Other pertinent metric	Other pertinent metric	Other pertinent metric	Other pertinent metric
List actions per member states and languages (see example table above)	Share cancel rate (%) following the unverified content label share warning pop-up (users who do not share the video after seeing the pop up)	Share of removals under misinformation policy	Share of proactive removals under misinformation policy	Share of video removals before any views under misinformation policy	Share of video removals within 24h by misinformation policy
Member States					
Austria	32.08%	39.66%	94.66%	79.97%	83.39%
Belgium	22.45%	64.65%	98.80%	74.80%	41.83%
Bulgaria	27.31%	37.77%	93.74%	89.13%	93.12%
Croatia	27.56%	21.77%	94.51%	68.13%	76.56%
Cyprus	27.93%	24.50%	95.59%	68.45%	80.97%
Czech Republic	28.32%	13.65%	83.85%	80.86%	86.96%
Denmark	22.83%	58.95%	97.18%	79.03%	81.41%
Estonia	39.34%	20.54%	85.87%	73.91%	84.78%



Finland	24.05%	19.60%	86.58%	73.25%	78.02%
France	24.85%	58.76%	99.16%	83.85%	65.39%
Germany	34.57%	49.23%	92.50%	48.96%	29.43%
Greece	28.30%	37.24%	95.29%	86.49%	91.99%
Hungary	27.18%	39.99%	93.03%	88.81%	94.03%
Ireland	25.86%	60.15%	97.11%	75.44%	56.67%
Italy	26.83%	57.32%	98.48%	85.26%	97.05%
Latvia	30.23%	22.27%	92.08%	87.55%	92.83%
Lithuania	28.32%	19.23%	97.27%	91.80%	93.36%
Luxembourg	28.83%	28.40%	97.63%	63.31%	59.76%
Malta	28.17%	32.28%	97.06%	83.33%	84.31%
Netherlands	23.46%	22.66%	95.83%	80.85%	72.97%
Poland	29.19%	31.26%	91.28%	71.34%	60.18%
Portugal	28.48%	30.78%	94.29%	85.64%	89.08%
Romania	27.30%	51.19%	93.59%	78.24%	86.41%
Slovakia	20.61%	35.47%	59.50%	48.19%	61.31%
Slovenia	20.44%	34.83%	95.71%	82.21%	71.78%
Spain	28.53%	42.47%	98.38%	76.64%	85.38%
Sweden	26.00%	50.80%	97.67%	76.58%	61.11%
Iceland	28.57%	43.48%	86.00%	48.00%	66.00%



Liechtenstein	0.00%	0.00%	0.00%	0.00%	0.00%
Norway	25.88%	63.25%	96.36%	60.15%	70.93%
Total EU	28.93%	47.31%	96.76%	77.53%	72.09%
Total EEA	28.84%	47.49%	96.76%	77.79%	72.11%
Member States		Share of video removals under Civic and Election Integrity policy	Share of proactive video removals under Civic and Election Integrity policy	Share of video removals before any views under Civic and Election Integrity policy	Share of video removals within 24h under Civic and Election Integrity policy
Austria		3.55%	81.55%	81.97%	99.14%
Belgium		1.84%	90.14%	90.61%	98.59%
Bulgaria		4.36%	97.87%	97.87%	99.47%
Croatia		1.91%	100.00%	100.00%	95.83%
Cyprus		8.13%	99.30%	99.30%	100.00%
Czech Republic		9.34%	98.79%	98.60%	100.00%
Denmark		3.45%	78.20%	78.20%	100.00%
Estonia		5.80%	34.62%	34.62%	100.00%
Finland		21.04%	94.20%	94.20%	99.91%
France		0.97%	96.65%	96.49%	99.02%
Germany		1.20%	98.39%	98.39%	98.79%
Greece		3.41%	100.00%	100.00%	99.39%
Hungary		3.01%	92.27%	92.27%	100.00%



Ireland		2.18%	82.93%	82.93%	98.37%
Italy		2.63%	99.57%	99.46%	99.26%
Latvia		4.45%	47.17%	47.17%	100.00%
Lithuania		2.78%	81.08%	81.08%	100.00%
Luxembourg		1.85%	90.91%	90.91%	100.00%
Malta		3.80%	100.00%	100.00%	100.00%
Netherlands		3.10%	98.68%	98.46%	99.67%
Poland		2.29%	97.37%	94.97%	95.08%
Portugal		6.09%	94.68%	94.12%	99.16%
Romania		2.56%	99.14%	98.80%	99.49%
Slovakia		5.70%	78.87%	66.20%	70.42%
Slovenia		1.07%	100.00%	100.00%	100.00%
Spain		2.39%	99.43%	98.65%	98.94%
Sweden		2.29%	77.39%	78.70%	100.00%
Iceland		0.00%	0.00%	0.00%	0.00%
Liechtenstein		0.00%	0.00%	0.00%	0.00%
Norway		3.15%	75.13%	75.66%	98.94%
Total EU		2.55%	96.58%	96.22%	98.97%
Total EEA		2.56%	96.29%	95.94%	98.97%



SLI 21.1.2 - actions taken under measure 21.1	Methodology of data measurement: The number of videos tagged with the unverified content label is based on the country in which the video was posted. The share cancel rate (%) following the unverified content label share warning pop-up indicates the percentage of users who do not share a video after seeing the label pop up. This metric is based on the approximate location of the users that engaged with these tools.			
		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
List actions per member states and languages (see example table above)		Number of videos tagged with the unverified content label		Share cancel rate (%) following the unverified content label share warning pop-up (users who do not share the video after seeing the pop up)
Member States				
Austria		2,550		32.08%
Belgium		4,726		22.45%
Bulgaria		1,049		27.31%
Croatia		813		27.56%
Cyprus		828		27.93%
Czech Republic		880		28.32%
Denmark		4,454		22.83%



Estonia		545		39.34%
Finland		2,106		24.05%
France		7,521		24.85%
Germany		8,261		34.57%
Greece		1,459		28.30%
Hungary		968		27.18%
Ireland		2,371		25.86%
Italy		4,027		26.83%
Latvia		636		30.23%
Lithuania		639		28.32%
Luxembourg		794		28.83%
Malta		459		28.17%
Netherlands		4,737		23.46%
Poland		2,032		29.19%
Portugal		1,867		28.48%
Romania		2,006		27.30%
Slovakia		564		20.61%
Slovenia		641		20.44%
Spain		4,996		28.53%
Sweden		4,575		26.00%



Iceland		410		28.57%
Liechtenstein		48		0.00%
Norway		2,869		25.88%
Total EU		66504		28.93%
Total EEA		69831		28.84%

Measure 21.2	
QRE 21.2.1	<p>We have undertaken consultations with researchers from the Massachusetts Institute of Technology (US) and the University of Regina (Canada) in order to understand the effect of showing users accurate information after they interacted with a misinformation claim. We continue to consult on product initiatives, e.g., see below re Dr. David G. Rand from MIT and the design of our AI-generated content labels.</p> <p>We continue exploring ways in which we can leverage this research to consider how we engage with users who have interacted with harmful misinformation on our platform and direct them to authoritative information.</p>
Measure 21.3	
QRE 21.3.1	<p>As set out within our response to QRE 17.1.1, we apply our unverified content, state-controlled media, and AI-generated labels to certain content in order to empower our community by providing them with an additional layer of context. We ensure these labels are developed and deployed in line with scientific evidence by partnering with fact-checkers and working with external experts, including scientists, in the following ways:</p> <ul style="list-style-type: none"> Unverified content label. In 2021, we partnered with behavioural scientists, Irrational Labs, on the design and testing of the specialised prompts which encourage users to consider content which has been labelled as unverified, before sharing it, as detailed in QRE 17.1.1. On testing the prompts, Irrational Labs found

that viewers decreased the rate at which they shared videos by 24%, while likes on such unsubstantiated content also decreased by 7%. Their full report can be found [here](#).

As mentioned above, we partner with a number of IFCN accredited fact-checkers in Europe, who assist with assessing the accuracy of certain content on our platform. Where our fact-checking partners determine that a video is not able to be confirmed or their fact-checks are inconclusive (which is sometimes the case, particularly during unfolding events or emergencies), we may apply our unverified content label to the video.

- **State-controlled media label.** In the last year, we have started applying our state-controlled media label to accounts or content where there is evidence of clear editorial control and decision-making by members of the state. To inform our state-affiliated media policy and approach to making such designations, we met with more than 60 media experts, political scientists, academics, and representatives from international organizations and civil society across North and South America, Africa, Europe, the Middle East, Asia, and Australia and will continue to work with these experts to inform our global approach and expansion of the policy.

As mentioned above, one of the experts we worked closely with was [Irrational Labs](#). In collaboration with their behavioural scientists, we considered the ways in which we could present the label to our users. As part of these efforts, we tested various copy options across English, Spanish, and Arabic via quantitative surveys and qualitative panels, and found that "[country] state-controlled media" was the option most preferred by users while being the most accurate representation of the relevant media entities' relationship to their respective governments.

- **AI-generated content label.** In advance of launching our new [AI-generated labels](#) for creators to disclose content that is completely AI-generated or significantly edited by AI, we consulted with our Safety Advisory Councils as well as industry experts including MIT's Dr. David G. Rand, who is studying how viewers perceive different types of AI labels. Dr. Rand's research helped guide the design of our AI-generated labels.

We are also continuously taking user feedback into consideration in order to identify new topics and consider which tools may be best suited to raising awareness around that topic and combating harmful misinformation.



V. Empowering Users	
Commitment 22	
<p>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.</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]	No
If yes, list these implementation measures here [short bullet points].	<ul style="list-style-type: none"> • TikTok did not subscribe to this commitment.
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?	<ul style="list-style-type: none"> • Aiming to build products and processes to more quickly launch user education interventions when a new crisis emerges.
Measure 22.1	
QRE 22.1.1	<p>Not committed. TikTok considers that the implementation of the other commitments under the Code (including, but not limited to, the other commitments relating to empowering users and fact-checking) provide a comprehensive approach to tackling disinformation, including facilitating users in making more informed decisions when they encounter online information that may be false or misleading. This position is also reflected in the Commission's guidance. As such, TikTok does not consider that committing to this measure will materially add to the other measures being adopted under the Code.</p>



	TikTok does, however, keep an open mind. As such, it is prepared to explore such solutions with the relevant providers in due course and to reassess whether such an approach would be beneficial, taking into account existing measures in place.
SLI 22.1.1 - actions enforcing policies above	N/A
	N/A
Member States	
Austria	
Belgium	
Bulgaria	
Croatia	
Cyprus	
Czech Republic	
Denmark	
Estonia	
Finland	
France	
Germany	
Greece	
Hungary	
Ireland	



Italy	
Latvia	
Lithuania	
Luxembourg	
Malta	
Netherlands	
Poland	
Portugal	
Romania	
Slovakia	
Slovenia	
Spain	
Sweden	
Iceland	
Liechtenstein	
Norway	
Total EU	
Total EEA	

Measure 22.2	
--------------	--



<p>QRE 22.2.1</p>	<p>Not committed. TikTok does not consider this to be a practical or implementable proposal. In any event, this measure is unnecessary as the combination of other commitments underpinning the Code (including, but not limited to, those relating to fact-checking) represent a comprehensive approach to achieving the goal of providing users with tools to make more informed decisions when they encounter online information that may be false or misleading.</p>
<p>Measure 22.3</p>	
<p>QRE 22.3.1</p>	<p>Not committed. Not relevant, linked to the above Measures.</p>
<p>Measure 22.4</p>	
<p>QRE 22.4.1</p>	<p>Not committed. Measures 22.4, 22.5 and 22.6 are not applicable as TikTok is not a provider of trustworthiness indicators.</p>
<p>SLI 22.4.1 - actions enforcing policies above</p>	<p>N/A</p>
	<p>N/A</p>
<p>Data</p>	<p>Not committed. TikTok does not consider this to be a practical or implementable proposal. In any event, this measure is unnecessary as the combination of other commitments underpinning the Code (including, but not limited to, those relating to fact-checking) represent a comprehensive approach to achieving the goal of providing users with tools to make more informed decisions when they encounter online information that may be false or misleading.</p>



Measure 22.5	
QRE 22.5.1	Not committed. Not relevant, linked to the above Measures.
SLI 22.5.1 - actions enforcing policies above	Not committed. Measures 22.4, 22.5 and 22.6 are not applicable as TikTok is not a provider of trustworthiness indicators.
Member States	
Austria	
Belgium	
Bulgaria	
Croatia	
Cyprus	
Czech Republic	
Denmark	
Estonia	
Finland	
France	
Germany	
Greece	
Hungary	



Ireland	
Italy	
Latvia	
Lithuania	
Luxembourg	
Malta	
Netherlands	
Poland	
Portugal	
Romania	
Slovakia	
Slovenia	
Spain	
Sweden	
Iceland	
Liechtenstein	
Norway	
Total EU	
Total EEA	



SLI 22.5.2 - actions enforcing policies above	N/A			
	N/A			
Data				
Measure 22.6				
QRE 22.6.1	Not committed. Measures 22.4, 22.5 and 22.6 are not applicable as TikTok is not a provider of trustworthiness indicators.			
SLI 22.6.1 - actions enforcing policies above	N/A			
	N/A			
Data				
Measure 22.7				
QRE 22.7.1	As per our response to QRE 17.1.1, we have numerous tools (including video notice tags, search interventions, public service announcements, in-app information centers and Safety Center pages) that lead users to authoritative sources available in all EU member states and in 23 official EU languages (plus, for EEA users, Norwegian and Icelandic). We also run localised campaigns on specific topics which deploy different engagement techniques depending on the subject matter and / or member state involved, e.g., in-person workshops, radio and newspaper campaigns.			
SLI 22.7.1 - actions enforcing policies above	N/A			
Member States				
Austria				



Belgium				
Bulgaria				
Croatia				
Cyprus				
Czech Republic				
Denmark				
Estonia				
Finland				
France				
Germany				
Greece				
Hungary				
Ireland				
Italy				
Latvia				
Lithuania				
Luxembourg				
Malta				
Netherlands				
Poland				



Portugal				
Romania				
Slovakia				
Slovenia				
Spain				
Sweden				
Iceland				
Liechtenstein				
Norway				
Total EU				
Total EEA				

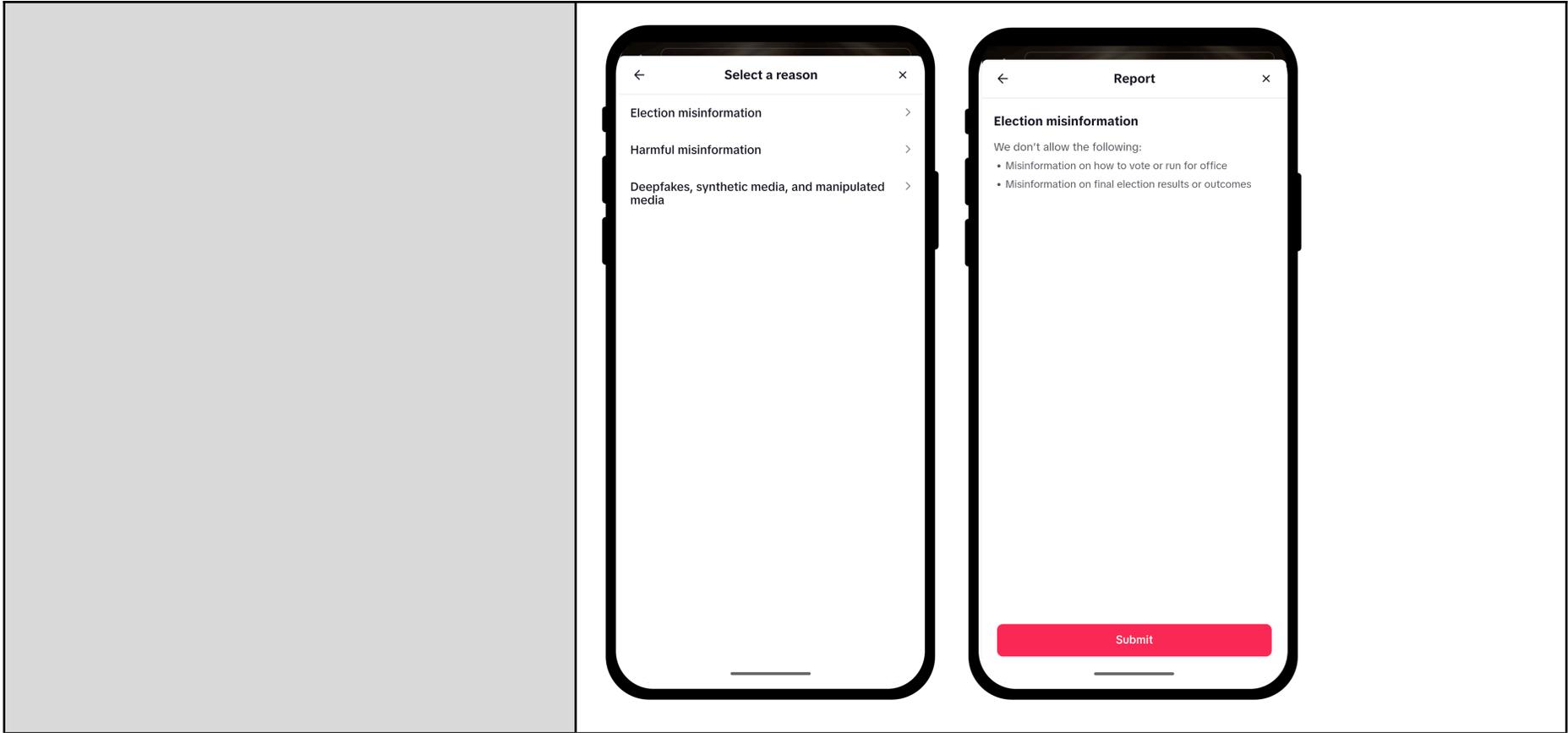
V. Empowering Users	
Commitment 23	
Relevant Signatories commit to provide users with the functionality to flag harmful false and/or misleading information that violates Signatories policies or terms of service.	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes



<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> • In line with our DSA requirements, we continue to provide an additional reporting channel for our community in the European Union to ‘Report Illegal Content,’ which enables users to alert us to content they believe breaches the law. • Improved transparency in relation to our appeals processes for users who disagree with the outcome of an illegal content report. • Continued investing in resources and training for our misinformation moderators and expanded our specialist misinformation moderation teams in the 11 countries in which we have added fact-checking partnerships.
<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]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> • Ensuring fact-checking coverage by a combination of permanent and temporary partnerships covering at least one official language of each of the European Member States ahead of the EU Elections. We will be expanding our misinformation moderation teams’ coverage accordingly.
<p>Measure 23.1</p>	
<p>QRE 23.1.1</p>	<p>We provide users with simple, intuitive ways to report/flag content in-app for any breach of our Terms of Service or CGs including for harmful misinformation in each EU Member State and in an official language of the European Union.</p> <ul style="list-style-type: none"> • By ‘long-pressing’ (e.g., clicking for 3 seconds) on the video content and selecting the “Report” option. • By selecting the “Share” button available on the right-hand side of the video content and then selecting the “Report” option.



	<p>The user is then shown categories of reporting reasons from which to select (which align with the harms our CGs seek to address). We recently updated this feature to make the “Misinformation” categories more intuitive and to allow users to report with increased granularity. We have also made changes to implement an additional option to enable users to report illegal content in line with our requirements under the DSA.</p>
--	--





Harmful misinformation

We don't allow the following:

- Misinformation that poses a risk to public safety or may cause panic, such as using old footage of a past event and falsely presenting it as current, or spreading inaccurate claims that essential items like food or water are no longer available
- Medical misinformation that poses a risk to public health, such as misleading statements about vaccines, and inaccurate medical advice that discourages people from getting appropriate medical care
- Climate change misinformation that contradicts well-established scientific consensus, such as denying the existence of climate change
- Dangerous conspiracy theories that promote violence, hatred, or target individuals, such as those causing prejudice toward a specific group and cause harm

Submit

Deepfakes, synthetic media, and manipulated media

We don't allow the following:

- Synthetic or manipulated media showing realistic scenes that are not prominently disclosed or labeled in the video
- Synthetic media that contains the likeness (visual or audio) of a real person when used for political or commercial endorsements, or if violative of our community guidelines
- Material that has been edited in a way that may mislead a person about real-world events
- Synthetic media showing a public figure in artistic and educational contexts, such as a celebrity doing a popular dance, and a historical figure featured in a history lesson, is allowed.

Submit

Users do not need to be logged into an account on the platform to report content, and can also report video content via the TikTok website (by clicking on the “Report” button which is prominently displayed in the upper right hand corner of each video when hovering over a video) or by means of our “Report Inappropriate content” webform which is available in our [Support Centre](#).

We are aware that harmful misinformation is not limited to video content and so users can also report a comment, a suggested search, a hashtag, a sound or an account, again specifically for harmful misinformation.



<p>Measure 23.2</p>	
<p>QRE 23.2.1</p>	<p>Reporting system</p> <p>To ensure the integrity of our reporting system, we deploy a combination of automated review and human moderation.</p> <p>Videos uploaded to TikTok are initially reviewed by our automated moderation technology, which aims to identify content that violates our Community Guidelines. If a potential violation of our CGs is found, the automated review system will either pass it on to our moderation teams for further review or, if there is a high degree of confidence that the content violates our CGs, remove it automatically. Automated removal is only applied when violations are clear-cut, such as where the content contains nudity or pertains to youth safety. We are continually working to improve the precision of our automated moderation technology so we can more effectively remove violative content at scale, while also reducing the number of incorrect removals.</p> <p>To support the fair and consistent review of potentially violative content, where violations are less clear-cut, content will be passed to our human moderation teams for further review. Human moderators can take additional context and nuance into account, which cannot always be picked up by technology, and in the context of harmful misinformation, for example, our moderators have access to a repository of previously fact-checked claims to help make swift and accurate decisions and direct access to our fact-checking partners who help assess the accuracy of new content.</p> <p>We have sought to make our CGs as clear and comprehensive as possible and have put in place robust Quality Assurance processes (including steps such as review of moderation cases, flows, appeals and undertaking Root Cause Analyses).</p> <p>As part of our requirements under the DSA, we have introduced an additional reporting channel for our community in the European Union to ‘Report Illegal Content,’ which enables users to alert us to content they believe breaches the law. TikTok will review the content against our CGs and where a violation is detected, the content may be removed globally. If it is not removed, our illegal content moderation team will further review the content to assess whether it is unlawful in the relevant jurisdiction - this assessment is undertaken by human review. If it is, access to that content will be restricted in that country. Those who report suspected illegal content will be notified of our decision, including if we consider that the content is not illegal. Users who disagree can appeal those decisions using the appeals process.</p>



	<p>We also note that whilst user reports are important, at TikTok we place considerable emphasis on proactive detection to remove violative content. We are proud that the vast majority of removed content is identified proactively before it is reported to us.</p> <p><u>Appeals system</u></p> <p>We are transparent with users in relation to appeals. We set out the options that may be available both to the user who reported the content and the creator of the affected content, where they disagree with the decision we have taken.</p> <p>The integrity of our appeals systems is reinforced by the involvement of our trained human moderators, who can take context and nuance into consideration when deciding whether content is illegal or violates our CGs.</p> <p>Our moderators review all appeals raised in relation to removed videos, removed comments, and banned accounts and assess them against our policies. To ensure consistency within this process and its overall integrity, we have sought to make our policies as clear and comprehensive as possible and have put in place robust Quality Assurance processes (including steps such as auditing appeals and undertaking Root Cause Analyses).</p> <p>If users who have submitted an appeal are still not satisfied with our decision, they can share feedback with us via the webform on TikTok.com. We continuously take user feedback into consideration to identify areas of improvement, including within the appeals process. Users may also have other legal rights in relation to decisions we make, as set out further here.</p>
--	--

<h2>V. Empowering Users</h2>
<h3>Commitment 24</h3>
<p>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.</p>



<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]</p>	<p>Yes</p>
<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> • Improved the user notification received following action on a user’s account or content to include further granularity on the action taken and a simple way to appeal the decision taken. • Improved user transparency around our appeals processes (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]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> • Continuing to review our user notification and appeal process and consider any feedback received from users and stakeholders on its user
<p>Measure 24.1</p>	
<p>QRE 24.1.1</p>	<p>Users in all EU member states are notified by an in-app notification in their relevant local language where the following action is taken:</p> <ul style="list-style-type: none"> • removal or otherwise restriction of access to their content; • a ban of the account; • restriction of their access to a feature (such as LIVE); or • restriction of their ability to monetise. <p>Such notifications are provided in near real time after action has been taken (i.e. generally within several seconds or up to a few minutes at most).</p>



	<p>Where we have taken any of these decisions, an in-app inbox notification sets out the violation deemed to have taken place, along with an option for users to “disagree” and submit an appeal. Users can submit appeals within 180 days of being notified of the decision they want to appeal. Further information, including about how to appeal a report is set out here.</p> <p>All such appeals raised will be queued for review by our specialised human moderators so as to ensure that context is adequately taken into account in reaching a determination. Users can monitor the status and view the results of their appeal within their in-app inbox.</p> <p>As mentioned above, our users have the ability to share feedback with us to the extent that they don't agree with the result of their appeal. They can do so by using the in-app function which allows them to "report a problem". We are continuously taking user feedback into consideration in order to identify areas of improvement within the appeals process.</p>			
SLI 24.1.1 - enforcement actions	Methodology of data measurement: The number of appeals/overturns is based on the country in which the video being appealed/overturned was posted. These numbers are only related to our Misinformation and Civic and Election Integrity policies.			
	Nr of enforcement actions	Nr of actions appealed	Metrics on results of appeals	
Member States				
List actions per member states and languages (see example table above)	Number of accounts removed banned under our I&A policies	Number of appeals of videos removed for violation of misinformation policy	Number of successful appeals for violation of misinformation policy (i.e. overturns)	
Member States				
Austria	149	354	131	



Belgium	300	1,473	920	
Bulgaria	112	151	111	
Croatia	145	34	25	
Cyprus	59	114	68	
Czech Republic	116	458	322	
Denmark	113	204	134	
Estonia	20	18	14	
Finland	150	152	98	
France	2,097	12,357	7,976	
Germany	2,720	7,071	2,021	
Greece	187	962	648	
Hungary	103	503	427	
Ireland	267	845	581	
Italy	1,792	5,356	4,554	
Latvia	39	38	36	
Lithuania	29	80	77	
Luxembourg	13	26	21	



Malta	5	10	8	
Netherlands	457	1,608	1,095	
Poland	1,735	3,175	1,894	
Portugal	111	249	176	
Romania	531	1,563	1,002	
Slovakia	63	104	61	
Slovenia	20	18	12	
Spain	1,278	5,949	4,137	
Sweden	276	1,217	639	
Iceland	27	13	10	
Liechtenstein	0	0	0	
Norway	337	329	213	
Total EU	12887	44089	27188	
Total EEA	13251	44431	27411	
List actions per member states and languages (see example table above)		Number of Appeals of videos removed for violation of Civic and Election Integrity policy	Number of overturns of appeals for violation of Civic and Election Integrity policy	



Member States				
Austria		13	12	
Belgium		16	16	
Bulgaria		18	18	
Croatia		0	0	
Cyprus		0	0	
Czech Republic		21	18	
Denmark		14	14	
Estonia		0	0	
Finland		8	8	
France		104	53	
Germany		54	51	
Greece		54	49	
Hungary		26	24	
Ireland		21	19	
Italy		267	253	
Latvia		4	4	



Lithuania		2	2	
Luxembourg		0	0	
Malta		0	0	
Netherlands		125	119	
Poland		169	159	
Portugal		30	29	
Romania		56	50	
Slovakia		2	2	
Slovenia		0	0	
Spain		173	166	
Sweden		17	11	
Iceland		0	0	
Liechtenstein		0	0	
Norway		21	17	
Total EU		1,194	1,077	
Total EEA		1,215	1,094	



V. Empowering Users	
Commitment 25	
<p>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.</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]	No
If yes, list these implementation measures here [short bullet points].	This commitment is not applicable as TikTok is not a messaging app.
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?	This commitment is not applicable as TikTok is not a messaging app.
Measure 25.1	
QRE 25.1.1	Not committed. This commitment is not applicable as TikTok is not a messaging app.
SLI 25.1.1	N/A
	N/A



Data	
Measure 25.2	
QRE 25.2.1	Not committed. This commitment is not applicable as TikTok is not a messaging app.
SLI 25.2.1 - use of select tools	N/A
	N/A
Data	



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.

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].	<ul style="list-style-type: none"> ● Expanded our Research API to Europe, which supports independent research through access to public data about TikTok content and accounts. ● Continued to make available the Commercial Content API in Europe to bring transparency to paid advertising, advertisers and other commercial content on TikTok. ● Opened our Commercial Content Library, a publicly searchable EU ads database with information about paid ads and ad metadata, such as the advertising creative, dates the ad ran, main parameters used for targeting (e.g. age, gender), number of people who were served the ad, and more.
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?	<ul style="list-style-type: none"> ● Continuing to receive feedback from researchers on their use of the Research and Commercial Content APIs and to make updates to better support independent research and enhance transparency about TikTok content.



	<ul style="list-style-type: none"> Continuing to expand and enhance the Research API.
<p>Measure 26.1</p>	
<p>QRE 26.1.1</p>	<p>We have a dedicated TikTok Transparency Centre available in a number of EU languages which hosts our:</p> <ul style="list-style-type: none"> COPD Transparency Reports. As part of our commitments to the Code, we publish a transparency report every six months to provide granular data, including approximately 2,600 metrics, for EU/EEA countries about our efforts to combat online misinformation. TikTok Community Guidelines Enforcement Reports. We provide proactive quarterly insights into the volume and nature of content and accounts removed from our platform for violating our Community Guidelines, Terms of Service or Advertising Policies since 2019. DSA Transparency Reports. Building on our proactive approach to transparency in our quarterly TikTok Community Guidelines Enforcement Reports and our obligations under the Digital Services Act (“DSA”), we publish a transparency report every six months to provide granular data for EU countries about our content moderation activities. <p>As part of our commitment to regulatory transparency and accountability, we also launched a new European Online Safety Hub, which will ultimately be available in 23 different European languages and serves as a 'one-stop-shop' for our community to learn more about how we're complying with the DSA.</p> <p>Our dedicated TikTok for Developers website hosts our Research and Commercial Content APIs (detailed below).</p>
<p>QRE 26.1.2</p>	<p>In our September 2023 Code report, TikTok has continued to disclose detailed data amounting to 2,600 metrics, covering 30 EEA member states over the entire H12023 period. We worked hard to both address outstanding data gaps, and further increase transparency by disclosing an additional 100 new metrics in certain areas. In this latest report, we are pleased to confirm that we are continuing these efforts and remain committed to increasing transparency around our metrics.</p> <p>We also provide ongoing insights into the action we take against content and accounts that violate our Community Guidelines (CGs), Terms of Service or Advertising Policies in our quarterly TikTok Community Guideline Enforcement Reports. The report includes a variety of</p>



	<p>data visualisations, which we recently updated to make it easier to read and understand, including for people with colour vision deficiency. We work hard to supplement the comprehensive data in the report and provide new insights. For example, we recently shared data on our response time to community-reported content and added information on TikTok LIVE enforcement. As part of our continued efforts to make it easy to study the TikTok platform, the report also offers access to aggregated data in a downloadable data file, which we recently expanded to include additional removal data by policy category for the 50 markets with the highest volumes of removed content.</p> <p>We provide access to researchers to data that is publicly available on our platform through our Research API and relating to commercial content through our Commercial Content API (detailed below).</p>		
SLI 26.1.1 - uptake of the tools and processes described in Measure 26.1			
Data			
Measure 26.2			
QRE 26.2.1	<p>(I) Research API</p> <p>To make it easier to independently research our platform and bring transparency to TikTok content, we built a Research API that provides researchers with access to public data on accounts and content, including comments, captions, subtitles, and number of comments, shares, likes, and favourites that a video receives, on our platform. More information is available here. We released an initial version of the Research API to academic researchers in the US and it has now been expanded to the EEA, UK and Switzerland. We have carefully considered feedback from researchers who have used the API and we have already made improvements including streamlining the application process, and enabling collaboration through Lab Access, allowing up to 10 researchers to work together on a shared research project.</p> <p>(II) Commercial Content API</p> <p>As required under the DSA, and to enhance transparency on advertisements presented on our platform, we have built a commercial content related API that includes ads, ad and advertiser metadata, and targeting information. Researchers and professionals are required to create a</p>		



	<p>TikTok Developers account and submit an application to access the Commercial Content API which we review to help prevent malicious actors from misusing this data.</p> <p>(III) Commercial Content Library</p> <p>The Commercial Content Library is a publicly searchable database with information about paid ads and ad metadata, such as the advertising creative, dates the ad ran, main parameters used for targeting (e.g. age, gender), number of people who were served the ad, and more. It also includes information about content that's commercial in nature and tagged with either a paid partnership label or promotional label, such as content that promotes a brand, product or service, but is not a paid ad.</p>
<p>QRE 26.2.2</p>	<p>See our response to QRE 26.1.1.</p> <p>(I) Research API</p> <p>Through our Research API, academic researchers from non-profit universities in the US and Europe can apply to study public data about TikTok content and accounts. This public data includes comments, captions, subtitles, and number of comments, shares, likes, and favourites that a video receives. More information is available here.</p> <p>(II) Commercial Content API</p> <p>Through our Commercial Content API, qualifying researchers and professionals can access data about commercial content in Europe including ads, ad and advertiser metadata, and targeting information.</p> <p>(II) Commercial Content Library</p> <p>Through our Commercial Content Library, the public can access information about paid ads and ad metadata, such as the advertising creative, dates the ad ran, main parameters used for targeting (e.g. age, gender), number of people who were served the ad, and more. It also includes information about content that's commercial in nature and tagged with either a paid partnership label or promotional label, such as content that promotes a brand, product or service, but is not a paid ad. The Commercial Content Library currently includes information on ads available to users in the European Economic Area (EEA), Switzerland, and the UK only.</p>



<p>QRE 26.2.3</p>	<p>For both our Research API and Commercial Content API, we make detailed information available to applicants through our dedicated website TikTok for Developers, on what data is made available and how to apply for access.</p> <p>Under the Research API, and once their application has been approved, we provide step-by-step instructions for researchers on how to access research data, how to comply with the security steps, and how to run queries on the data.</p> <p>Similarly with the Commercial Content API, we provide participants with detailed information on how to query ad data and fetch public advertiser data.</p>					
<p>SLI 26.2.1 - meaningful metrics on the uptake, swiftness, and acceptance level of the tools and processes in Measure 26.2</p>	<p>Research and Commercial Content APIs</p> <p>Since launching, in Europe, we have received 167 applications to the TikTok Research API from non-profit academic researchers in the EEA on topics related to consumer trends, misinformation, mental health and more and 57 applications to access the TikTok Commercial Content API.</p> <p>Commercial Content Library</p> <p>During the reporting period, there were 50,291 unique EEA visitors to the Commercial Content Library.</p>					
	<p>Number of applications received for Researchers API</p>	<p>Number of applications accepted for Researchers API</p>	<p>Number of applications rejected for Researchers API</p>	<p>Number of applications received for TikTok Commercial Content API</p>	<p>Number of applications accepted for TikTok Commercial Content API</p>	<p>Number of applications rejected for TikTok Commercial Content API</p>
<p>Austria</p>	<p>10</p>	<p>2</p>	<p>3</p>	<p>1</p>	<p>1</p>	<p>0</p>
<p>Belgium</p>	<p>4</p>	<p>2</p>	<p>1</p>	<p>0</p>	<p>0</p>	<p>0</p>
<p>Bulgaria</p>	<p>0</p>	<p>0</p>	<p>0</p>	<p>0</p>	<p>0</p>	<p>0</p>
<p>Croatia</p>	<p>0</p>	<p>0</p>	<p>0</p>	<p>0</p>	<p>0</p>	<p>0</p>
<p>Cyprus</p>	<p>1</p>	<p>0</p>	<p>0</p>	<p>1</p>	<p>0</p>	<p>1</p>



Czech Republic	1	0	1	1	1	0
Denmark	10	6	1	3	2	1
Estonia	0	0	0	1	1	0
Finland	6	1	2	0	0	0
France	18	2	10	11	11	0
Germany	27	11	6	13	13	0
Greece	4	1	2	1	1	0
Hungary	2	1	0	0	0	0
Ireland	1	1	0	0	0	0
Italy	19	4	9	2	2	0
Latvia	0	0	0	0	0	0
Lithuania	0	0	0	1	1	0
Luxembourg	0	0	0	0	0	0
Malta	0	0	0	0	0	0
Netherlands	20	8	3	3	3	0
Poland	2	0	2	5	2	3
Portugal	3	1	2	1	1	0
Romania	1	0	0	1	1	0
Slovakia	1	0	1	0	0	0
Slovenia	0	0	0	0	0	0
Spain	26	9	10	10	10	0



Sweden	2	0	1	4	3	1
Iceland	0	0	0	0	0	0
Lichtenstein	0	0	0	0	0	0
Norway	9	4	1	0	0	0
EU Level	143	45	50	57	52	5
EEA Level	152	49	51	57	52	5
Measure 26.3						
QRE 26.3.1	<p>We welcome feedback from researchers on our APIs and have a dedicated support form where researchers can provide feedback about their experience. Prior to expanding the Research API to Europe, we acted on feedback from US based researchers and made improvements by streamlining the application process and enabling greater collaboration through Lab Access.</p>					

VI. Empowering the research community	
Commitment 27	
<p>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.</p>	
<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]</p>	<p>Yes</p>
<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> Participated in the data access pilot with EDMO trialling the process for sharing data with vetted researchers designated under the DSA.



	<ul style="list-style-type: none"> Actively participating in the EDMO working group for the creation of the Independent Intermediary Body (IIB) to support research on digital platforms. Contributed to the European Commission's Call for Evidence on Data Access under the DSA.
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?	<ul style="list-style-type: none"> Continue participating in the working group which has been setup to implement the Independent Intermediary Body (IIB). Building on work completed as part of the EDMO data access pilot, continuing preparations to provide data access to vetted researchers under the DSA
Measure 27.1	
QRE 27.1.1	<p>We have engaged with EDMO and are actively participating in the working group that has been set up in order to implement the Independent Intermediary Body (IIB).</p> <p>We participated in the data access pilot with EDMO trialling the process for sharing data with vetted researchers designated under the DSA. The pilot is aimed at informing the future processes around granting access to data under Article 40(4) DSA. TikTok was one of only two platforms to commit the requisite time and resources to partake in the pilot.</p> <p>TikTok also contributed to the European Commission's Call for Evidence on Data Access under the DSA. We submitted a comprehensive response reflecting feedback from cross-functional teams within TikTok, including from data scientists and privacy and to privacy experts.</p>
Measure 27.2	



QRE 27.2.1	We are participating in the working group which has been set up to implement the Independent Intermediary Body (IIB).
Measure 27.3	
QRE 27.3.1	We are participating in the working group which has been set up to implement the Independent Intermediary Body (IIB). TikTok participated in the data access pilot with EDMO trialling the process for sharing data with vetted researchers designated under the DSA.
SLI 27.3.1 - research projects vetted by the independent third-party body	N/A
	N/A
Data	
Measure 27.4	
QRE 27.4.1	We participated in the data access pilot with EDMO trialling the process for sharing data with vetted researchers designated under the DSA. We are one of the two platforms to commit the requisite time and resources to partake in the pilot. The pilot is aimed at informing the future processes around granting access to data under Article 40(4) DSA.

VI. Empowering the research community	
Commitment 28	
Relevant Signatories commit to support good faith research into Disinformation that involves their services.	
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



<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> • Expanding our Research API to Europe, which provides researchers with access to public data about TikTok content and accounts. • Continued to provide the Commercial Content API in Europe to bring transparency to paid advertising and other commercial content on TikTok. • Participated in the data access pilot with EDMO trialling the process for sharing data with vetted researchers as designated under the DSA.
<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]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> • Continuing to seek feedback from researchers on their use of the Research API and Commercial Content API and to make updates to better support independent research and transparency into TikTok. • Building on work completed as part of the data access pilot with EDMO, continuing preparations to provide data access to vetted researchers under the DSA. • Continuing to expand and enhance the Research API.
<p>Measure 28.1</p>	
<p>QRE 28.1.1</p>	<p>TikTok is committed to facilitating research and engaging with the research community.</p> <p>As set out above, TikTok is committed to facilitating research through our Research and Commercial Content APIs and Commercial Content Library, full details of which are available on our TikTok for Developers website. We have many teams and individuals across product, policy, data science, outreach and legal committing time and focus to facilitating research. We are actively working to expand and enhance the Research API.</p>



We are committed to leading the way when it comes to being transparent in how we operate, moderate and recommend content, and secure our platform. That's why we opened our global Transparency and Accountability Centers (**TACs**) for experts and lawmakers to see first-hand how we're working to build a safe and secure platform for our growing and diverse community. Our TACs, located in Dublin, Los Angeles, Singapore, and Washington DC, provide guests with opportunities to visit and see first-hand how teams at TikTok go about the critically important work of securing our community's safety, data, and privacy. In April 2023, the Dublin TAC was visited by 10 Irish NGOs working and conducting research in the online safety space. Later, in September 2023, the Dublin TAC welcomed a delegation of our European Fact-Checking partners.

In addition to these efforts, there are a plethora of ways through which we engage with the research community in the course of our work.

We work closely with our eight regional [Safety Advisory Councils](#), including our European Safety Advisory Council, which bring together a diverse array of independent experts from academia and civil society. Advisory Council members provide subject matter expertise and advice on issues relating to user safety, content policy, and emerging issues that affect TikTok and our community, most recently in the development of our new [AI-generated label](#) for creators to disclose content that is completely AI-generated or significantly edited by AI. These councils are an important way to bring outside perspectives into our company and onto our platform.

Our **Outreach & Partnerships Management Team** is dedicated to establishing partnerships and regularly engaging with civil society stakeholders and external experts, including the academic and research community, to ensure their perspectives inform our policy creation, feature development, risk mitigation, and safety strategies. For example, we engaged with numerous academics in Europe as part of the development and implementation of our state-affiliated media policy. We also worked closely with industry experts on our AI-generated content label, including MIT's Dr. David G. Rand, who is studying how viewers perceive different types of AI labels. Dr. Rand's research helped guide the design of our AI-generated labels.

More recently, we engaged with global experts on our Election Misinformation policies, which will help inform future updates of our I&A policies. This team also plays an important role in our efforts to counter misinformation by identifying, onboarding and managing new partners to our fact-checking programme, for example, Demagog in Poland and Poligrafo in Portugal in this latest reporting period.

In the lead-up to certain elections, for example in Spain (Newtral), Netherlands (DPA), Poland



	<p>(Demagog) and Slovakia (DigiQ) during this reporting period, we invite suitably qualified external local/regional experts, as part of our Election Speaker Series, to share their market expertise with our internal teams to provide us with insights to better understand areas that could potentially amount to election manipulation and to inform our approach to the upcoming election.</p> <p>TikTok teams and personnel also regularly participate in research-focused events. At the end of June 2023, TikTok sent a 12 strong delegation to GlobalFact10 in Seoul, South Korea. TikTok was one of three top-tier sponsors of GlobalFact10, the International Fact-Checking Network's largest gathering for professional fact-checkers. In addition to sponsorship, TikTok delivered a Main Stage Session presentation on our approach to misinformation and hosted a breakout session on how to create authoritative and engaging content on the platform.</p> <p>TikTok attended the Trust and Safety Research Conference at Stanford University in September 2023, where we hosted a Research API workshop for academics. In the workshop, academic researchers learned about TikTok's Research API and had the opportunity to walk through sample queries.</p> <p>In December 2023, TikTok conducted another workshop on the TikTok Research API hosted by Northeastern University's Co-Laboratory for Data Impact. There were about 20 participants composed of faculty and students from both Northeastern and Harvard University in the U.S. Also in December, we hosted a webinar organised by the French authority ARCOM to brief academic researchers in France on the expansion of our Research API to Europe.</p> <p>Other relevant examples include, the Terrorism and Social Media Conference (Swansea University), and the Association of Internet Researchers Conference (Philadelphia).</p> <p>As well as opportunities to share context about our approach, research interests, and opportunities to collaborate, these events enable us to learn from the important work being done by the research community on various topics, which include aspects related to harmful misinformation.</p>
Measure 28.2	
QRE 28.2.1	<p>We have a dedicated TikTok for Developers website which hosts APIs for our research information.</p> <p>With the Research API, researchers can access:</p>



	<ul style="list-style-type: none"> • Public account data, such as user profiles, comments, performance data, such as number of comments, likes, and favorites that the user receives; • Public content data, such as comments, captions, subtitles, performance data, such as number of comments, shares, likes, and favorites that the video receives; and • Public data for keywords search results. <p>Our commercial content related APIs includes ads, ad and advertiser metadata, and targeting information. These APIs will allow the public and researchers to perform customised - advertiser name or keyword based - searches on ads and other commercial content data that is stored in the Commercial Content Library repository. The Commercial Content Library is a searchable database with information about paid ads and ad metadata, such as the advertising creative, dates the ad ran, main parameters used for targeting (e.g. age, gender), number of people who were served the ad, and more.</p>
Measure 28.3	
QRE 28.3.1	We are eager to engage and cooperate with EDMO as part of this annual consultation and to receive feedback from the research community on how we facilitate their research projects on our platform.
Measure 28.4	
QRE 28.4.1	We are committed to regularly engage and collaborate with EDMO including our participation in the pilot trialling the process for sharing data with vetted researchers designated under the DSA and on the creation of the IIB.

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.



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].	This Commitment relates to Research Organisations.
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?	This Commitment relates to Research Organisations.
Measure 29.1	
QRE 29.1.1	Not committed.
QRE 29.1.2	Not committed.
QRE 29.1.3	Not committed.
SLI 29.1.1 - reach of stakeholders or citizens informed about the outcome of research projects	N/A
	N/A
Data	



Measure 29.2	
QRE 29.2.1	Not committed.
QRE 29.2.2	Not committed.
QRE 29.2.3	N/A
SLI 29.2.1	N/A
	Not committed.
Data	
Measure 29.3	
QRE 29.3.1	Not committed.
SLI 29.3.1 - reach of stakeholders or citizens informed about the outcome of research projects	N/A
	N/A
Data	



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

<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]</p>	<p>Yes</p>
<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> • Continued to scale-up our fact-checking program, expanding to two new EU countries (Croatia and Portugal) and expanding our misinformation moderation teams for those languages. • Onboarding two new local fact-checking partners Demagog (Poland) and Poligrafo (Portugal). • Sponsored the Global Fact 10 Global Fact-Checking Conference hosted by the International Fact-Checking Network in June 2023 and hosted a panel discussion on our approach to countering harmful misinformation. • Continued to expand our fact-checking repository to ensure our teams and systems leverage the full scope of insights our fact-checking partners submitted to TikTok (regardless of the original language of the relevant content). • Continued to explore ways to improve data sharing in connection with our pilot scheme to share enforcement data with our fact-checking partners on the claims they have provided feedback on. • Continued to conduct regular surveys with our partners to review our working relationship.



	<ul style="list-style-type: none"> Participated in the newly created working group within the Code framework on the creation of an external fact-checking repository.
<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]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> Ensuring fact-checking coverage by a combination of permanent and temporary partnerships covering at least one official language of each of the European Member States ahead of the EU Parliamentary Election in June 2024. As part of these plans, we will be expanding our misinformation moderation teams' coverage accordingly. Continuing to develop our fact-checking repository, as well as continuing to participate in the sub-group on the creation of an external repository. Further increasing the quality of our method of data sharing with fact-checking partners.
<p>Measure 30.1</p>	
<p>QRE 30.1.1</p>	<p>Within Europe, we work with 11 fact-checking partners who provide fact-checking coverage in 18 official EU languages. Our partners have teams of fact-checkers who review and verify reported content. Our moderators then use that independent feedback to take action and where appropriate, remove or make ineligible for recommendation false or misleading content or label unverified content.</p> <p>Our agreements with our partners are standardised, meaning the agreements are based on our template master services agreements and consistent with common standards and conditions. We review and update our template standard agreements as part of our annual contract renewal process.</p> <p>The terms of the agreements describe:</p> <ul style="list-style-type: none"> The service the fact-checking partner will provide, namely that their team of fact checkers review, assess and rate video content uploaded to their fact-checking queue.



	<ul style="list-style-type: none"> • The expected results e.g., the fact-checkers advise on whether the content may be or contain misinformation and rate it using our classification categories. • An option to agree that our fact-checker partners provide regular written reports about disinformation trends identified. • An option to receive pro-actively flagging of potential harmful misinformation from our partners. • The languages in which they will provide fact-checking services. • The ability to request temporary coverage regarding additional languages or support on ad hoc additional projects. • All other key terms including the applicable term and fees and payment arrangements.
<p>QRE 30.1.2</p>	<p>Within Europe, our IFCN-accredited fact-checking partners are:</p> <ol style="list-style-type: none"> 1. Agence France Press; 2. Facta.news; 3. Lead Stories; 4. Logically; 5. Newtral; 6. Science Feedback; 7. dpa Deutsche Presse-Agentur; 8. Reuters; 9. Demagog; 10. Poligrafo; and 11. Teyit. <p>We can, and have, put in place temporary agreements with these fact checking partners to provide additional European language coverage for a period in an unfolding crisis. For example, we put in place temporary fact-checking coverage in Serbia for the Serbian parliamentary election on 17 December 2023.</p> <p>Outside of our fact-checking program, we also collaborate with a variety of fact-checking partners to develop media literacy campaigns and work on other discrete projects. We have collaborated with Demagog, Facta, Fakenews.pl, Logically, Maldita and Newtral on localised media literacy campaigns. For example:</p> <ul style="list-style-type: none"> • 2023 Spanish election (23rd July). We worked with Newtral, our fact-checking partner, and Maldita, a local media literacy organisation, to produce educational videos about the electoral process and election misinformation.



	<ul style="list-style-type: none"> ● 2023 Polish election (15th Oct). We partnered with Demagog and FakeNews.pl to develop our media literacy strategy with the objective of educating users on how to detect misinformation and verify information they are seeing online. <p>Globally, we have 18 IFCN-accredited fact-checking partners. We are continuously working to expand our fact-checking network and we keep users updated on our efforts to do so here.</p>
<p>QRE 30.1.3</p>	<p>We have fact-checking coverage in 18 official European languages (Croatian, Dutch, English, French, German, Hungarian, Italian, Polish, Portuguese, Romanian, Spanish, Swedish, Danish, Finnish, Greek, Czech, Slovakian, and Bulgarian), and, therefore, the spoken language of 24 EEA countries.</p> <p>We have fact-checking coverage in a number of other European languages or languages which affect European users, including Norwegian, Russian and Ukrainian and we can request additional support in Azeri, Armenian, Turkish, and Belarusian.</p> <p>In terms of global fact-checking initiatives, we currently cover more than 50 languages and assess content in more than 100 countries, thereby improving the overall integrity of the service and benefiting European users. As mentioned, we are continuing to expand our fact-checking network in Europe and globally.</p> <p>In order to effectively scale the feedback provided by our fact-checkers globally, we have implemented the measures listed below.</p> <ul style="list-style-type: none"> ● Fact-checking repository. We have built a repository of previously fact-checked claims to help misinformation moderators make swift and accurate decisions. ● Trends reports. Our fact-checking partners can provide us with regular reports identifying general misinformation trends observed on our platform and across the industry generally, including new/changing industry or market trends, events or topics that generated particular misinformation or disinformation. ● Proactive detection by our fact-checking partners. Our fact-checking partners are authorised to proactively identify content that may constitute harmful misinformation on our platform and suggest prominent misinformation that is circulating online that may benefit from verification. ● Fact-checking guidelines. We create guidelines and trending topic reminders for our moderators on the basis of previous fact-checking assessments. This ensures our moderation teams leverage the insights from our fact-checking partners and helps our



	<p>moderators make swift and accurate decisions on flagged content regardless of the language in which the original claim was made.</p> <ul style="list-style-type: none"> Election Speaker Series. To further promote election integrity, and inform our approach to country-level EU elections, we invited suitably qualified local and regional external experts to share their insights and market expertise with our internal teams. Our recent election speaker series heard presentations from our local fact-checking partners including Newtral for Spain, Demagog for Poland, and DPA for Netherlands. <p>Members of moderation teams receive specialised training on misinformation and have direct access to these tools and measures, which enables them to more accurately take action on violating content across Europe and globally.</p> <p>We are continuing to invest in building, and improving, models which may allow for the output of these measures to be used to update the machine learning models we use in proactive detection, learning, over time, to search for similar content which can be proactively recalled into our moderation system for review. We use a variety of automated tools, including:</p> <ul style="list-style-type: none"> Computer Vision models, which help to detect objects so it can be determined whether the content likely contains material which violates our policies. Keyword lists and models, which are used to review text and audio content to detect material in violation of our policies. We work with various external experts, including our fact-checking partners, to inform our keyword lists. Where we have previously detected content that violates our policies, we use de-duplication and hashing technologies that enable us to recognise copies or near copies of such content to prevent further re-distribution of violative content on our platform. <p>Continuing to leverage the fact-checking output in this way enables us to further increase the positive impact of our fact checking programme.</p>
SLI 30.1.1 - Member States and languages covered by agreements with the fact-checking organisations	
Austria	Fact-checking coverage implemented
Belgium	Fact-checking coverage implemented



Bulgaria	Fact-checking coverage implemented
Croatia	Fact-checking coverage implemented
Cyprus	Fact-checking coverage implemented
Czech Republic	Fact-checking coverage implemented
Denmark	Fact-checking coverage implemented
Estonia	We are working hard to continue to expand our fact-checking programme. Meanwhile, our fact-checking repository and other initiatives benefit all European users and ensure the overall integrity of our platform.
Finland	Fact-checking coverage implemented
France	Fact-checking coverage implemented
Germany	Fact-checking coverage implemented
Greece	Fact-checking coverage implemented
Hungary	Fact-checking coverage implemented
Ireland	Fact-checking coverage implemented
Italy	Fact-checking coverage implemented
Latvia	We are working hard to continue to expand our fact-checking programme. Meanwhile, our fact-checking repository and other initiatives benefit all European users and ensure the overall integrity of our platform.
Lithuania	
Luxembourg	Fact-checking coverage implemented



Malta	We are working hard to continue to expand our fact-checking programme. Meanwhile, our fact-checking repository and other initiatives benefit all European users and ensure the overall integrity of our platform.
Netherlands	Fact-checking coverage implemented
Poland	Fact-checking coverage implemented
Portugal	Fact-checking coverage implemented
Romania	Fact-checking coverage implemented
Slovakia	Fact-checking coverage implemented
Slovenia	We are working hard to continue to expand our fact-checking programme. Meanwhile, our fact-checking repository and other initiatives benefit all European users and ensure the overall integrity of our platform.
Spain	Fact-checking coverage implemented
Sweden	Fact-checking coverage implemented
Iceland	We are working hard to continue to expand our fact-checking programme. Meanwhile, our fact-checking repository and other initiatives benefit all European users and ensure the overall integrity of our platform.
Liechtenstein	Fact-checking coverage implemented
Norway	Fact-checking coverage implemented
Total EU	22
Total EEA	24



Measure 30.2	
QRE 30.2.1	<p>Our agreements with our fact-checking partners are standardised, meaning the agreements are based on our template master services agreements and consistent of common standards and conditions. These agreements, as with all of our agreements, must meet the ethical and professional standards we set internally including containing anti-bribery and corruption provisions.</p> <p>Our partners are compensated in a fair, transparent way based on the work done by them using standardised rates. Our fact-checking partners then invoice us on a monthly basis based on work done.</p> <p>All of our fact-checking partners are independent organisations, which are certified through the non-partisan IFCN. Our agreements with them explicitly state that the fact-checkers are non-exclusive, independent contractors of TikTok who retain editorial independence in relation to the fact-checking services that they provide, and that the services shall be performed in a professional manner and in line with the highest standards in the industry. Our processes are also set up to ensure our fact-checking partners independence. Our partners access flagged content through an exclusive dashboard for their use and provide their assessment of the accuracy of the content by providing a rating. Fact-checkers will do so independently from us, and their review may include calling sources, consulting public data or authenticating videos and images.</p> <p>To facilitate transparency and openness with our fact-checking partners, we regularly meet with them to provide data regarding their feedback and also to conduct surveys.</p>
QRE 30.2.2	<p>We meet regularly with our fact-checking partners and have an ongoing dialogue with them about how our partnership is working and evolving. We survey our fact-checking partners to encourage feedback about what we are doing well and how we could improve.</p> <p>We are continuing to share fact-checking enforcement data with our fact-checking partners. Impact assessments are currently shared on a bimonthly basis. Going forward, we are exploring potential ways to further increase the quality of our methods of data sharing with fact-checking partners.</p>
QRE 30.2.3	This provision is not relevant to TikTok, only to fact-checking organisations.



Measure 30.3	
QRE 30.3.1	<p>Given our fact-checking partners are all IFCN-accredited, our fact-checking partners already engage in some informal cross-border collaboration through that network.</p> <p>In addition, we continue to collaborate with our partners to understand how we may be able to facilitate further collaboration. In September 2023, we held a roundtable discussion with a number of our fact-checking partners across the EMEA region. The purpose of the discussions was to provide our fact-checking partners with information about our procedures - in particular, our end-to-end moderation process (of which they form an integral part), I&A policy development, and CG enforcements. As part of this roundtable, we held a session which included a session on how to collaborate in the context of the upcoming EU elections.</p>
Measure 30.4	
QRE 30.4.1	<p>We are in regular dialogue with EDMO and the EFCSN on these and other issues. We continue to be open to discussing and exploring what further progress can be made on these points.</p>

VII. Empowering the fact-checking community	
Commitment 31	
<p>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.</p>	
<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]</p>	<p>Yes</p>
<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> Expanded our fact-checking coverage to 2 further EEA countries (Croatia and Portugal),



	<p>and in parallel, expanded our misinformation moderation teams for those languages.</p> <ul style="list-style-type: none"> • Hosted a roundtable discussion over 2 days in September 2023 with a number of our fact-checking partners in the EMEA region, which included a session on how to collaborate in the context of the upcoming EU elections. • Continued to expand our fact-checking repository to ensure our teams and systems leverage the full scope of insights our fact-checking partners submitted to TikTok (regardless of the original language of the relevant content). • Participated in the newly created working group within the Code framework on the creation of an external fact-checking repository.
<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]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> • Ensuring fact-checking coverage by a combination of permanent and temporary partnerships covering at least one official language of each of the European Member States ahead of the European Parliamentary Election in June 2024. As part of these plans, we will be expanding our misinformation moderation teams' coverage accordingly. • Continuing to develop our fact-checking repository and tools for fact-checking. • Continue to work with the relevant working group to create an external repository of fact-checking content.
<p>Measure 31.1</p>	
<p>Measure 31.2</p>	



QRE 31.1.1

We see harmful misinformation as different from other content issues. Context and fact-checking are critical to consistently and accurately enforcing our harmful misinformation policies, which is why we work with 11 fact-checking partners in Europe, covering 18 official European languages.

While we use machine learning models to help detect potential misinformation, our approach is to have members of our content moderation team, who receive specialised training on misinformation, assess, confirm, and take action on harmful misinformation. This includes direct access to our fact-checking partners who help assess the accuracy of content. Our fact-checking partners are involved in our moderation process in three ways:

- I. A moderator sends a video to fact-checkers for review and their assessment of the accuracy of the content by providing a rating. Fact-checkers will do so independently from us, and their review may include calling sources, consulting public data, authenticating videos and images, and more.

While content is being fact-checked or when content can't be substantiated through fact-checking, we may reduce the content's distribution so that fewer people see it. Fact-checkers ultimately do not take action on the content directly. The moderator will instead take into account the fact-checkers' feedback on the accuracy of the content when deciding whether the content violates our CGs and what action to take.

- II. Contributing to our global database of previously fact-checked claims to help our misinformation moderators make decisions.
- III. A proactive detection programme with our fact-checkers who flag new and evolving claims that they are seeing on our platform. This enables our moderators to quickly assess these claims and remove violations.

In addition, we use fact-checking feedback to provide additional context to users about certain content. As mentioned, when our fact checking partners conclude that the fact-check is inconclusive or content is not able to be confirmed, (which is especially common during unfolding events or crises), we inform viewers [via a banner](#) when we identify a video with unverified content in an effort to raise users' awareness about the credibility of the content and to reduce sharing. The video may also become ineligible for recommendation into other user's For You feed to limit the spread of potentially misleading information.

In September 2023, we held a roundtable discussion with a number of our fact-checking partners across the EMEA region. The purpose of the discussions was to provide our fact-checking partners with information about our procedures - in particular, our end-to-end



	<p>moderation process (of which they form an integral part), I&A policy development, and Community Guidelines enforcements. As part of this roundtable, we held a session which included a discussion on how to collaborate in the context of the upcoming EU elections.</p> <p>As we have substantially expanded our fact-checking network and the period upon which we are reporting, there has been a corresponding increase in market coverage that we are able to report on. We are also working internally to develop metrics which meaningfully demonstrate the impact of our fact-checking programme across Europe.</p>			
SLI 31.1.1 - use of fact-checks	<p>Methodology of data measurement:</p> <p>The number of fact checked videos is based on the number of videos that have been sent for review to one of our fact-checking partners in the relevant territory.</p>			
	Nr of fact-checked articles published			
List actions per member states and languages (see example table above)	Number of fact checked videos (tasks)			
Member States				
Austria	15			
Belgium	893			
Bulgaria	160			
Croatia	83			
Cyprus	42			
Czech Republic	54			
Denmark	119			
Estonia	0			



Finland	64			
France	2,313			
Germany	474			
Greece	131			
Hungary	7			
Ireland	15			
Italy	270			
Latvia	2			
Lithuania	2			
Luxembourg	2			
Malta	0			
Netherlands	61			
Poland	458			
Portugal	30			
Romania	2,699			
Slovakia	34			
Slovenia	6			
Spain	452			
Sweden	640			
Iceland	0			



Liechtenstein	0			
Norway	542			
Total EU	9,026			
Total EEA	9,568			

SLI 31.1.2 - impact of actions taken	Methodology of data measurement:		
	<p>The number of videos removed as a result of a fact checking assessment and the number of videos removed because of policy guidelines, known misinformation trends and our knowledge based repository is based on the country in which the video was posted.</p> <p>These metrics correspond to the numbers of removals under the harmful misinformation policy since all of its enforcement are based on the policy guidelines, known misinformation trends and knowledge based repository.</p>		
	N/A		
List actions per member states and languages (see example table above)	Number of videos removed as a result of a fact checking assessment	Number of videos removed because of policy guidelines, known misinformation trends and knowledge based repository	
Member States			
Austria	0	2,601	
Belgium	129	7,481	
Bulgaria	12	1,629	
Croatia	22	273	
Cyprus	7	431	



Czech Republic	5	2,408	
Denmark	13	2,270	
Estonia	0	92	
Finland	6	1,028	
France	674	74,537	
Germany	105	30,460	
Greece	15	7,106	
Hungary	2	3,100	
Ireland	6	3,388	
Italy	54	55,954	
Latvia	1	265	
Lithuania	1	256	
Luxembourg	0	169	
Malta	0	102	
Netherlands	7	6,663	
Poland	154	11,955	
Portugal	10	1,804	
Romania	776	11,671	
Slovakia	2	442	
Slovenia	2	163	



Spain	83	25,053	
Sweden	124	5,099	
Iceland	0	50	
Liechtenstein	0	0	
Norway	105	3,794	
Total EU	2,210	256,400	
Total EEA	2,315	260,244	

SLI 31.1.3 – Quantitative information used for contextualisation for the SLIs 31.1.1 / 31.1.2	Methodology of data measurement: The metric we have provided demonstrates the % of videos which have been removed as a result of the fact checking assessment, in comparison to the total number of videos removed because of violation of our misinformation policy.
List actions per member states and languages (see example table above)	Number of videos removed as a result of a fact checking assessment / number of removals under misinformation policy
Austria	0.00%
Belgium	1.72%
Bulgaria	0.74%
Croatia	8.06%



Cyprus	1.62%
Czech Republic	0.21%
Denmark	0.57%
Estonia	0.00%
Finland	0.58%
France	0.90%
Germany	0.34%
Greece	0.21%
Hungary	0.06%
Ireland	0.18%
Italy	0.10%
Latvia	0.38%
Lithuania	0.39%
Luxembourg	0.00%
Malta	0.00%
Netherlands	0.11%
Poland	1.29%
Portugal	0.55%
Romania	6.65%
Slovakia	0.45%



Slovenia	1.23%
Spain	0.33%
Sweden	2.43%
Iceland	0.00%
Liechtenstein	0.00%
Norway	2.77%
Total EU	0.86%
Total EEA	0.89%

Measure 31.3	
QRE 31.3.1	We are participating in the sub-group newly created for this purpose. We actively worked with all signatories to define clear deliverables and timelines for the creation of an external fact-checking repository, as contemplated in this measure.
Measure 31.4	
QRE 31.4.1	We commit to being an active participant in the discussion about technological solutions to facilitate the efficient use of the common repository across platforms and languages.

VII. Empowering the fact-checking community
Commitment 32



<p>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.</p>	
<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]</p>	<p>Yes</p>
<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> Continued to explore ways to improve data sharing in connection with our pilot scheme to share enforcement data with our fact-checking partners on the claims they have provided feedback on.
<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]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> Further increasing the quality of our methods of data sharing with fact-checking partners.
<p>Measure 32.1</p>	
<p>Measure 32.2</p>	
<p>QRE 32.1.1</p>	<p>Our fact-checking partners access content which has been flagged for review through a dashboard made available for their exclusive use. The dashboard shows our fact-checkers certain quantitative information about the services they provide, including the number of videos queued for assessment at any one time, as well as the time the review has taken. Fact-checkers can also use the dashboard to see the rating they applied to videos they have previously assessed.</p> <p>We are continuing to share fact-checking enforcement data with our fact checking partners, where we give our partners bimonthly feedback to help them quantify the impact of the</p>



	<p>fact-checked content over time e.g., the number of videos removed as a result of their feedback. This initiative has been well-received among our partners.</p> <p>Going forward, we plan to continue to explore ways to further increase the quality of our methods of data sharing with fact-checking partners.</p>
<p>SLI 32.1.1 - use of the interfaces and other tools</p>	<p>Methodology of data measurement:</p> <p>N/A. As mentioned in our response to QRE 32.1.1, the dashboard we currently share with our partners only contains high level quantitative information about the services they provide, including the number of videos queued for assessment at any one time, as well as the time the review has taken. We are continuing to work with our fact checking partners to understand what further data it would be helpful for us to share with them.</p>
<p>Data</p>	
<p>Measure 32.3</p>	
<p>QRE 32.3.1</p>	<p>We continue to participate in the taskforce made up of the relevant signatories' representatives that is being set up for this purpose. Meanwhile we are also engaging with EDMO pro-actively on this commitment.</p>

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.



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].	This Commitment and Measure relates to fact-checking organisations.
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?	This Commitment and Measure relates to fact-checking organisations.
Measure 33.1	
QRE 33.1.1	Not committed. This Commitment and Measure relates to fact-checking organisations.
SLI 33.1.1 - number of European fact-checkers that are IFCN-certified	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]	Yes
If yes, list these implementation measures here [short bullet points].	<ul style="list-style-type: none"> We have been an active participant in the working group that has successfully launched the common Transparency Centre this year. We also took up the position of co-chair of the Transparency working group in September 2023.
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?	<ul style="list-style-type: none"> We are committed to furthering the efforts of the Transparency working group in our role as co-chair, and to building on the successful launch of the common Transparency Centre by collecting feedback from stakeholders in order to drive future improvements.
Measure 34.1	
Measure 34.2	
Measure 34.3	
Measure 34.4	



Measure 34.5	
--------------	--

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].	<ul style="list-style-type: none"> • Through our participation in the working group that has successfully launched the common Transparency Centre this year, we have ensured that the Centre will allow the general public to access general information about the Code as well as the underlying reports (and for the Centre to be navigated both by commitment and signatory). • We have supported the working group in collecting feedback on the user experience of the website. We have engaged with the vendor to increase the robustness of the website and make improvements to the interface.
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?	<ul style="list-style-type: none"> • We are committed to furthering the efforts of the Transparency working group in our role as co-chair, and to building on the successful launch of the common Transparency Centre by collecting feedback from key stakeholders in order to guide future improvements.



Measure 35.1	
Measure 35.2	
Measure 35.3	
Measure 35.4	
Measure 35.5	
Measure 35.6	

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].	<ul style="list-style-type: none"> • We have supported the working group in collecting feedback on the user experience of the website.
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



<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> We are committed to maintaining the common Transparency Centre and, as part of this, updating the requisite information in a timely and complete manner.
<p>Measure 36.1</p>	
<p>Measure 36.2</p>	
<p>Measure 36.3</p>	
<p>QRE 36.1.1 (for the Commitments 34-36)</p>	<p>We are pleased to confirm that we have been an active participant in the working group that has successfully launched the common Transparency Centre this year. We have assisted with establishing the website's requirements, selecting a vendor to build the website and overseeing the development of the website's key functionalities and interface. We have ensured that the Centre will allow the general public to access general information about the Code as well as the underlying reports (and for the Centre to be navigated both by commitment and signatory). Each signatory will be responsible for ensuring that the information they upload to the website is correct and accurate. Entities interested in joining the Code's Task-force will be able to sign up through a dedicated online application form on the website. We have supported the working group in collecting feedback on the user experience of the website and will continue to seek such feedback from relevant stakeholders to better maintain and update the website.</p>
<p>QRE 36.1.2 (for the Commitments 34-36)</p>	<p>We are committed to maintaining the website and supporting the development of relevant SLIs. 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.</p>
<p>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.</p>	<p>We are working with the vendor to support the development of relevant metrics for this SLI.</p>
<p>Data</p>	<p>The common Transparency Center has received around 35,000 views globally between 1 July 2023 and 31 December 31 2023. The average engagement time on the website is 1m 11s and reports have been downloaded more than 9,000 times.</p>



IX. Permanent Task-Force Commitment 37



IX. Permanent Task-Force

Commitment 37

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

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].	<ul style="list-style-type: none"> We have meaningfully engaged in the Task-force and all of its working groups and subgroups. We have joined new relevant groups when created, such as the Elections working group which TikTok co-chairs, as well as the Generative AI working group.
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?	<ul style="list-style-type: none"> We will continue to engage in the Task-force and all of its working groups and subgroups.
Measure 37.1	
Measure 37.2	
Measure 37.3	
Measure 37.4	
Measure 37.5	



<p>Measure 37.6</p>	
<p>QRE 37.6.1</p>	<p>We have meaningfully engaged in the Task-force and all of its working groups and subgroups:</p> <ul style="list-style-type: none"> ● Monitoring and Reporting ● Integrity of Services ● Crisis Response ● Transparency Centre ● Outreach and Integration ● Ad Scrutiny ● Empowerment of Fact-Checkers ● Elections ● Generative AI <p>We will continue to engage in the Task-force and all of its working groups and subgroups.</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].	<ul style="list-style-type: none"> Globally more than 40,000 Trust and Safety professionals are dedicated to keeping TikTok safe.
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?	<ul style="list-style-type: none"> Continue to dedicate resources in line with our ongoing obligations under the Code.
Measure 38.1	
QRE 38.1.1	<p>TikTok has assigned the highest priority level to the Code, which means that we have, and will continue to have, appropriate resources in place to meet our commitments and compliance.</p> <p>Given the breadth of the Code and the commitments therein, our work spans multiple teams, including Trust and Safety, Legal, Monetisation Integrity, Product and Public Policy. Teams across the globe are deployed to ensure that we meet our commitments and compliance with the notable involvement of our Trust and Safety Leadership team which is based in Dublin, Ireland.</p>



	<p>As of September 2023, TikTok has more than 6,000 people dedicated to the moderation of content in the European Union, as we recognise the importance of local knowledge and expertise as we work to ensure online safety for our users. We take a similar approach to our third party partnerships.</p>
--	--

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.

<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]</p>	<p>Yes</p>
<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> • We have shared our second report with the Commission in accordance with the agreed timeframes.
<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]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> • We are committed to continue to report on our Code commitments on a regular basis within the agreed timeframes.

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]	Yes
If yes, list these implementation measures here [short bullet points].	<ul style="list-style-type: none"> We have reported on the SLIs and QREs relevant to the Commitments we signed-up to within this report at a level of detail beyond any previous transparency efforts.
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?	<ul style="list-style-type: none"> We are committed to reporting on the SLIs and QREs relevant to the Commitments we signed-up to in line with the timeframes agreed.
Measure 40.1	
Measure 40.2	
Measure 40.3	
Measure 40.4	
Measure 40.5	



Measure 40.6	
--------------	--

X. Monitoring of Code

Commitment 41

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

In 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].	<ul style="list-style-type: none"> • We have been an active participant in the working group dedicated to developing Structural Indicators. • We supported the publication of pilot Structural Indicators by TrustLab, through our collaboration with EDMO, ERGA, Avaaz and the European Commission.
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?	<ul style="list-style-type: none"> • We will continue to support the publication of Structural Indicators, and work towards further honing their methodology and scope.



Measure 41.1	
Measure 41.2	
Measure 41.3	

X. Monitoring of Code	
Commitment 42	
<p>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.</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].	<ul style="list-style-type: none"> We have been an active participant in the Crisis Response working group and have shared reports specific to the War of aggression by Russia on Ukraine, the Israel/Hamas conflict and the 2024 Elections for the European Parliament along with this report.
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?	<ul style="list-style-type: none"> We will continue to participate in the Crisis Response working group and share reports on topics aligned upon.



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].	<ul style="list-style-type: none"> • Participated in the monitoring and reporting working group. • Provided timely feedback on the harmonized reporting template.
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?	<ul style="list-style-type: none"> • We will continue to participate in the working group and contribute feedback to the report template.

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	



<p>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.</p>	
<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]</p>	<p>Yes</p>
<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> • TikTok is committed to meeting its obligations under the DSA, including the independent audit obligations. We have taken steps to ensure readiness for our audit obligations and have appointed an external independent auditor to assess our compliance with these obligations.
<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]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> • TikTok will publish the DSA audit report that will result from the independent auditor's compliance assessment in due time. TikTok is committed to audit its compliance with its COPD Commitments as soon as the COPD becomes a Code of Conduct under the DSA.



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

Reporting on the service's response during a crisis

War of aggression by Russia on Ukraine

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

The war of aggression by Russia on Ukraine (hereinafter, “**War in Ukraine**”) is devastating, and, as a platform, has challenged us to confront a complex and rapidly changing environment. At TikTok, the safety of our people and community is of paramount importance and we work continuously to safeguard our platform.

We have set out below some of the main threats we have observed on our platform in relation to the spread of harmful misinformation and covert influence operations (**CIO**) related to the war and note that we are committed to taking action to prevent such content from being shared in this context.

(I) Spread of harmful misinformation

We continue to observe and take action where appropriate under our policies. In terms of trends observed, we have seen false or unconfirmed claims about specific attacks and events, the development or use of weapons, the involvement of specific countries in the conflict and statements about specific military activities, such as the direction of troop movement. We also have seen instances of footage repurposed in a misleading way, including from video games or unrelated footage from past events presented as current.

As detailed below, we take a multi-faceted approach to understanding and removing misleading stories and, when it comes to addressing harmful misinformation, we apply the [Integrity & Authenticity policies \(I&A policies\)](#) in our [Community Guidelines \(CGs\)](#) and we will take action on such content from our platform. We support our moderation teams with detailed policy guidance and direction when moderating on crisis related misinformation using our misinformation policies, including providing case banks of harmful misinformation claims to support their moderation work.

(II) CIOs

We fight against CIO as our I&A policies prohibit attempts to sway public opinion while also misleading our systems or users about the identity, origin, approximate location, popularity or overall purpose. We have specifically-trained teams which are on high alert to investigate and detect CIO on our platform.

We have confirmed that during the period from April to September 2023, we took action to remove a total of 7 networks (consisting of 16,281 accounts in total) that were found to be involved in coordinated attempts to influence public opinion about the War in Ukraine while also misleading individuals, our community, or our systems. We publish all of the CIO networks we identify and remove within our transparency reports, [here](#).

We know that CIO will continue to evolve in response to our detection and networks may attempt to re-establish a presence on our platform, which is why we continually seek to strengthen our policies and enforcement actions in order to protect our community against new types of harmful misinformation and inauthentic behaviours.



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

We are continually working hard to ensure that TikTok is a source of reliable and safe information and recognise the heightened risk and impact of misleading information during a time of crisis.

(I) Investment in our fact-checking program

We employ a layered approach to detecting harmful misinformation which is in violation of our CGs. In order to ensure coverage which is comprehensive and responsive to the war, we have invested in Russian and Ukrainian native language speakers for content moderation, as we recognise the importance of local cultural and linguistic context within the process.

Working closely with our fact-checking partners has been a crucial part of our approach to enforcing harmful misinformation on our platform. Our fact-checking programme includes coverage in Russia, Ukraine and Belarus. As part of the scale-up of our fact checking program, we have onboarded Reuters, who are dedicated to fact-checking content in Russian and Ukrainian. Since the beginning of the War in Ukraine, we have also leveraged Ukrainian-speaking reporters who are connected with some of our existing fact checking partners to further support our fact-checking efforts in Ukraine specifically.

Collaborating with certain of our fact-checking partners to receive advance warning of emerging misinformation narratives has facilitated proactive responses against high-harm trends and has ensured that our moderation teams have up-to-date guidance.

(II) Disruption of CIOs

Disrupting CIO networks has also been high priority work for us in the context of the crisis and we published a list of the networks we disrupted in the relevant period within our most recently published transparency report, [here](#).

Between September 2022 and March 2023, we took action to remove a total of 7 networks (consisting of 16,281 accounts in total) that were found to be involved in coordinated attempts to influence public opinion about the War in Ukraine while also misleading individuals, our community, or our systems. We publish all of the CIO networks we identify and remove within our transparency reports, [here](#).

(III) Restricting access to content for state affiliated media

Since the early stages of the war, we have restricted access to content from a number of Russian state affiliated media entities in the EU, Iceland and Liechtenstein. We also expedited the rollout of our state affiliated media policy to bring viewers context to evaluate the content they consume on our platform and labels have since been applied to content posted by the accounts of such entities in Russia, Ukraine and Belarus.

Since January 2023, we have scaled up our detection and labelling of state-controlled media accounts following the roll-out of our state-controlled media



label policy globally. We are committed to further expansion.

(IV) Mitigating the risk of monetisation of harmful misinformation

Whilst we have long prohibited political advertising on our platform, we have taken measures to further mitigate the risk of monetisation off the back of the War in Ukraine by disallowing Ukrainian and Russian advertisers from targeting EU markets and removing Livestream videos originating Ukraine from the For You feed of users located in the EU. The ability to add new video content or Livestream videos to the platform in Russia also continues to be suspended.

(V) Launching localised media literacy campaigns

Lastly, recognising the importance of proactive measures which are aimed at improving our users' digital literacy and increasing the prominence of authoritative information, during the last six months, we launched six localised media literacy campaigns addressing disinformation related to the War in Ukraine in Austria, Bulgaria, Czech Republic, Croatia, Germany and Slovenia, in close collaboration with our fact-checking partners. Users searching for keywords relating to the War in Ukraine are directed to tips, prepared in partnership with our fact checking partners, to help users identify misinformation and prevent the spread of it on the platform.

[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
Integrity and Authenticity Policies	We continue to rely on our existing, robust I&A policies, which are an effective basis for	In the context of the War in Ukraine, we have been able to rely on our I&A policies, which are our first line of defence in combating harmful misinformation and deceptive behaviours on our platform. These guidelines make clear to our users what content we remove or make ineligible for the For You feed when they pose a risk of harm to our users or the wider public. We have also supported our moderation teams with detailed policy guidance and direction when moderating on war-related



	<p>tackling content related to the war.</p> <p>As such, we have not needed to introduce new policies, or adapt our Terms of Service or CGs, for the purposes of addressing the crisis.</p> <p>In a crisis, we keep under review our policies and to ensure moderation teams have supplementary guidance.</p>	<p>harmful misinformation using existing policies.</p> <p>We have specialist teams within our Trust and Safety department dedicated to the policy issue of I&A, including within the areas of product and policy. Our experienced subject matter experts on I&A continually keep these policies under review and collaborate with external partners and experts when understanding whether updates are required.</p> <p>When situations such as the War in Ukraine arise, these teams work to ensure that appropriate guidance is developed so that the I&A policies are applied in an effective manner in respect of content relating to the relevant crisis (in this case, the War in Ukraine). This includes issuing detailed policy guidance and direction, including providing case banks on harmful misinformation claims to support moderation teams.</p>
<p>Scrutiny of Ads Placements</p>		
<p>Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.</p>		
<p>Preventing misuse of our monetisation features</p> <p>(Commitment 1, Measure 1.1)</p>	<p>Description of intervention</p> <p>Since the beginning of the War in Ukraine, we have taken a strict position not to enable associated monetisation. This includes direct monetisation (e.g. the sale of merchandise associated with the war) as well as any reference to the War in Ukraine. Since March 2022, we have not allowed Ukrainian and Russian based advertisers to target EU markets.</p> <hr/> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>N/A</p>	



<p>Content moderation (Commitment 2, Measure 2.2)</p>	<p>Description of intervention</p> <p>We use a combination of automated and human moderation in order to identify content that breaches our ad policies.</p> <p>We enforce our ad policies with a combination of automated and human moderation, and have expert teams focused on investigating and responding to any attempts to circumvent our policies.</p> <p>Our Monetisation Integrity department has moderation teams in multiple locations that speak Russian and Ukrainian.</p> <hr/> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>Given the range of potential policy violations that could be engaged, we are currently unable to provide metrics specific to this issue.</p>
<p>Political Advertising</p>	
<p>Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.</p>	
<p>Prohibition on Political Advertising (Commitment 4)</p>	<p>Description of intervention</p> <p>In an effort to maintain both the integrity of the platform and safety of the people who use it, accounts belonging to politicians or political parties are not able to advertise or make money on TikTok.</p> <p>We do not allow paid political promotion, political advertising, or fundraising by politicians and political parties (for themselves or others). Our political ads policy includes both traditional paid ads and creators receiving compensation to support or oppose a candidate for office. This has been a long-standing policy at TikTok since 2019. We don't allow paid or branded content that promotes or opposes a candidate, current leader, political party or group, or issue at the federal, state, or local level – including election-related ads, advocacy ads, or issue ads.</p> <hr/> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>Our monetisation integrity content teams observed a sharp rise in attempts to post ads related to political/war content during the initial period of the conflict commencement. Our risk control methods ensured there was no corresponding increase in</p>



	<p>violating activity going live on the platform. Since the initial period of the conflict, these numbers have significantly dropped. We have since seen no additional spike.</p>
<p>Integrity of Services</p>	
<p>Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.</p>	
<p>Identifying and removing CIO networks (Commitment 14, Measure 14.1)</p>	<p>Description of intervention</p> <p>We fight against CIO as our I&A policies prohibit attempts to sway public opinion while also misleading our systems or users about the identity, origin, approximate location, popularity or overall purpose. Our dedicated investigation teams and automated systems have been on high alert to identify threats related to CIO networks and have removed networks targeting discourse about the War in Ukraine, in accordance with our I&A policies which prohibit deceptive behaviours.</p> <p>We know that CIO will continue to evolve in response to our detection and networks may attempt to re-establish a presence on our platform, which is why we continually seek to strengthen our policies and enforcement actions in order to protect our community against new types of harmful misinformation and inauthentic behaviours.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>NB: We are only able to provide the Q2 and Q3 2023. Data on Q4 2022 and Q1 2023 is available in our previous Crisis Report. We are building and testing data infrastructure that can provide information requested at a high level of fidelity. Additionally, CIO network investigations are highly resource heavy requiring in depth analysis to ensure high confidence in proposed actions. We publish all of the CIO networks we identify and remove within our transparency reports, here.</p> <p>Between April to September 2023, we took action to remove a total of 7 networks (consisting of 16,281 accounts in total) that were found to be involved in coordinated attempts to influence public opinion about the Russia-Ukraine war while also misleading individuals, our community, or our systems.</p> <p>We published this information within our most recently published transparency report, here.</p> <p>The following networks targeting discourse around the War in Ukraine were removed between April and September 2023:</p>



In Q2 2023:

- We assess that this network operated from Russia and targeted Russian audiences in Russia, Netherlands, Romania, France and the UK. The individuals behind this network created inauthentic accounts and hyper-posted content in order to artificially amplify specific pro-Russia viewpoints in the context of the war in Ukraine, circumventing the regional TikTok ban in Russia
 - Accounts in network: 588
 - Followers of network: 36,331

In Q3 2023:

- We assess that this network operated from Russia and targeted a European audience, including Germany and Ukraine. The individuals behind this network created a large number of inauthentic accounts in order to covertly amplify pro-Russian foreign policy viewpoints in Europe within the context of the war between Russia and Ukraine.
 - Accounts in network: 12,820
 - Followers of network: 847,760
- We assess that this network operated from Ukraine and targeted a Ukrainian audience. The individuals behind this network created inauthentic accounts and posted content at scale, in Ukrainian, artificially amplifying narratives aiming to raise money for the Ukrainian military.
 - Accounts in network: 2,350
 - Followers of network: 81,570
- We assess that this network operated from Ukraine and targeted a Ukrainian audience. The individuals behind this network created inauthentic accounts in order to amplify misinformation videos, targeting discourse about the ongoing war between Russia and Ukraine.
 - Accounts in network: 302
 - Followers of network: 57,806
- We assess that this network operated from Russia and targeted Russian and Ukrainian audiences, as well as the Russian speaking audience in Europe. The individuals behind this network created inauthentic accounts in order to artificially amplify pro-Russian narratives, targeting discourse about the ongoing war between Russia and Ukraine.
 - Accounts in network: 133
 - Followers of network: 199,569
- We assess that this network operated from Slovakia and targeted a Slovakian audience. The individuals behind this network created opaque accounts which engaged in inauthentic audience building methods in order to inauthentically amplify anti-EU, anti-NATO and pro-Russian content in Slovakia.



	<ul style="list-style-type: none"> ○ Accounts in network: 69 ○ Followers of network: 2,154 <ul style="list-style-type: none"> ● We assess that this network operated from Russia and targeted users from Germany, Italy, Turkey, Serbia, Czechia, Poland and Greece using local languages. The individuals behind this network created inauthentic accounts, including fictitious news agencies in order to artificially amplify pro-Russian narratives, targeting the ongoing war between Russia and Ukraine. <ul style="list-style-type: none"> ○ Accounts in network: 19 ○ Followers of network: 217,008
<p>Tackling synthetic and manipulated media</p> <p><i>(Commitments 14 and 15, Measures 14.1, 15.1 and 15.2)</i></p>	<p>Description of intervention</p> <p>We do not allow synthetic media (AI-generated audio and visual content) content on the platform that may mislead our users or cause harm.</p> <p>Our Synthetic and Manipulated Media Policy requires deceptive or synthetic media that shows realistic scenes be clearly disclosed.</p> <p>On September 19, 2023, we launched a new AI-generated content label for creators to disclose content that is completely AI-generated or significantly edited by AI. For the purposes of our policy, synthetic media refers to content created or modified by AI technology. It includes highly realistic digitally-created (fake) content of real people, such as a video of a real person speaking but their words have been modified or changed.</p> <p>Prohibited practices are set out in our I&A policies here.</p> <hr/> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>Our efforts support transparent and responsible content creation practices, both in the context of the War in Ukraine and more broadly on our platform.</p>
<p>Removing harmful misinformation from our platform</p>	<p>Description of intervention</p> <p>We take action to remove accounts or content which contain inaccurate, misleading, or false content that may cause</p>



<p>(Commitment 14, Measure 14.1)</p>	<p>significant harm to individuals or society, regardless of intent. In conflict environments, such information may include content that is repurposed from past conflicts, content which makes false and harmful claims about specific events, or incites panic. In certain circumstances, we may also reduce the prominence of such content.</p> <p>We employ a layered approach to misinformation detection, leveraging multiple overlapping strategies to ensure comprehensive and responsive coverage. We place considerable emphasis on proactive content moderation strategies in order to remove harmful misinformation which is in violation of our policies before it is reported to us by users or third parties.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>In the context of the crisis, we are proud to have proactively removed thousands of videos containing harmful misinformation related to the War in Ukraine. We have been able to do this through a combination of automated review, human level content moderation, carrying out targeted sweeps of certain types of content (e.g. hashtags/sensitive keyword lists) as well as working closely with our fact-checking partners and responding to emerging trends they identify.</p> <p>We have invested heavily in Russian and Ukrainian native language speakers for content moderation, as we recognise the importance of local cultural and linguistic context in the misinformation moderation process.</p> <p><i>Relevant metrics:</i></p> <ul style="list-style-type: none"> • Number of videos removed because of violation of misinformation policy with a proxy related to the War in Ukraine - 6,304 • Number of videos not recommended because of violation of misinformation policy with a proxy (only focusing on RU/UA) - 7,199 • Number of proactive removals of videos removed because of violation of misinformation policy with a proxy related to the War in Ukraine - 5,485
<p>Empowering Users</p>	
<p>Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.</p>	
<p>Not proactively promoting news-type content to our users</p>	<p><i>Description of intervention</i></p> <p>TikTok is primarily an entertainment platform. It may be the case that a user's For You feed shows more news-type content (such as news content relating to the War in Ukraine) over time if that is content that a user is actively looking for and</p>



<p>(Commitment 18, Measure 18.1)</p>	<p>engaging with, but we do not actively promote news content to users on TikTok.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>Our approach to news-type content supports our efforts to reduce the spread of harmful disinformation to users.</p>
<p>Removing Ukrainian Livestream content from the For You feed of EU users</p> <p>(Commitment 18, Measure 18.1)</p>	<p>Description of intervention</p> <p>We have removed Livestream videos originating in Ukraine from the For You feed of users located in the EU. This has been done in order to minimise the risk of harmful content appearing in a user's feed and given the uptick of Livestreams from that region since the outbreak of the War in Ukraine.</p> <p>We also swiftly took action to suspend new content creation from our video service in Russia in order to review the safety implications of the "fake news" law which was passed by the Russian parliament in March 2022.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>We have taken these actions to minimise the risk of harmful content appearing in a user's feed.</p>
<p>Applying our state affiliated media label</p> <p>(Commitment 17, Measure 17.1)</p>	<p>Description of intervention</p> <p>We have restricted access to certain state-affiliated media entities and expedited the roll-out of our state-affiliated media policy and label in order to bring viewers context to evaluate content shared by such Russian, Ukrainian and Belarusian entities.</p> <p>In the EU, Iceland and Liechtenstein, we have taken steps to restrict access to content from the following entities: Russia Today; Sputnik; Rossiya RTR/RTR Planeta; Rossiya 24/Russia 24; and TV Centre International.</p> <p>We have also rolled out our state-affiliated media policy in order to bring viewers context to evaluate the content they consume on our platform in relation to the war and labels have since been applied to content posted by the accounts of such entities in Russia, Ukraine and Belarus.</p> <p>Where the label is applied to content, users across the EEA are automatically shown a full screen pop-up containing</p>



	<p>information about what the label means and inviting the user to click on “learn more” and be redirected to an in-app page, which explains why the content has been labelled as state-controlled media.</p> <p><i>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</i></p> <p>Since January 2023, we have scaled up our detection and labelling of state-controlled media accounts following the roll-out of our state-controlled media label policy globally. We are committed to further expansion.</p> <p><i>Relevant metrics:</i></p> <ul style="list-style-type: none"> ● Number of videos tagged with the state affiliated media label for Russia, Belarus and Ukraine - 114,218 ● Number of impressions of the state affiliated media label for Russia, Belarus and Ukraine - 12,286,269
<p>Creating localised media literacy campaigns <i>(Commitment 17, Measures 17.2 and 17.3)</i></p>	<p><i>Description of intervention</i></p> <p>We recognise the importance of proactive measures which are aimed at improving our users' digital literacy and increasing the prominence of authoritative information.</p> <p>We launched localised media literacy campaigns relating to the crisis in order to raise awareness amongst our users. We promoted the campaign through a combination of our in-app intervention tools in order to ensure that authoritative information is promoted to our users.</p> <p>Users searching for keywords relating to the War in Ukraine are directed to tips, prepared in partnership with our fact checking partners, to help users identify misinformation and prevent the spread of it on the platform.</p> <p><i>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</i></p> <p>Working with our fact-checking partners, in the previous year we have developed and rolled-out six localised media literacy campaigns addressing disinformation related to the War in Ukraine in Austria, Bulgaria, Czech Republic, Croatia, Germany and Slovenia.</p> <p><i>Relevant metrics for the six media literacy campaigns (EEA total numbers):</i></p> <ul style="list-style-type: none"> ● Total Number of impressions of the search intervention - 16,105,548 ● Total Number of clicks on the search intervention - 83,585



	<ul style="list-style-type: none"> • Click through rate of the search intervention - 0.52%
Empowering the Research Community	
<p>Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.</p>	
Measures taken to support research into crisis related misinformation and disinformation <i>(Commitment 27, Measure 26.1 and 26.2)</i>	Description of intervention <p>Through our Research API, academic researchers from non-profit universities in the US and Europe can apply to study public data about TikTok content and accounts. This public data includes comments, captions, subtitles, and number of comments, shares, likes, and favourites that a video receives. More information is available here.</p>
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available <p>During the period of this COPD report, we have approved 2 applications to the Research API, with an express focus on the War in Ukraine.</p>
Empowering the Fact-Checking Community	
<p>Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.</p>	
Applying our unverified content label to make content ineligible for recommendation <i>(Commitment 31, Measure 31.2)</i>	Description of intervention <p>Where our misinformation moderators or fact-checking partners determine that content is not able to be verified at the given time (which is common during an unfolding event), we apply our unverified content label to the content to encourage users to consider the reliability or source of the content. The application of the label will also result in the content becoming ineligible for recommendation in order to limit the spread of potentially misleading information.</p>
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available



	<p>Verifying certain information during dynamic and fast moving events such as a war can be challenging and our moderators and fact-checkers cannot always conclusively determine whether content is indeed harmful misinformation, in violation of our CGs.</p> <p>Therefore, in order to minimise risk, where our fact-checkers or our trained moderators do not have enough information to verify content which may potentially be misleading, we apply our unverified content label to inform users the content has been reviewed but cannot be conclusively validated. The goal is to raise users' awareness about the credibility of the content and to reduce sharing (see screenshots here). Our unverified content label is available to users in 23 EU official languages (plus, for EEA users, Norwegian and Icelandic).</p> <p>Where the banner is applied, the content will also become ineligible for recommendation into anyone's For You feed to limit the spread of information relating to unfolding events where details are still developing and which may potentially be misleading.</p>
<p>Ensuring fact-checking coverage</p> <p><i>(Commitment 30, Measure 30.1)</i></p>	<p><i>Description of intervention</i></p> <p>Our fact checking efforts cover Russian, Ukrainian, Belarusian and all major European languages (including 18 official languages of the European Member States as well as a number of other languages which affect European users).</p> <hr/> <p><i>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</i></p> <p>We see harmful misinformation as different from other content issues. Context and fact-checking are critical to consistently and accurately enforcing our harmful misinformation policies, which is why we have ensured that, in the context of the crisis, our fact-checking programme covers Russian, Ukrainian and Belarusian.</p> <p>More generally, we work with 11-fact-checking partners in Europe, covering the spoken language of 22 EEA countries (as well as a number of other languages which affect European users). We recently onboarded a new fact-checking partner, Reuters, who are dedicated to fact-checking content in Russian and Ukrainian. To further support our fact-checking efforts in Ukraine specifically, we have also been leveraging additional Ukrainian-speaking reporters who are connected with some of our existing fact checking partners.</p> <p>We are committed to expanding our fact-checking program by on-boarding new European-based fact-checking partners and increasing our operational coverage in the EEA (and expanding our misinformation moderation teams accordingly).</p> <p><i>Relevant metrics:</i></p>



	<ul style="list-style-type: none"> • Number of fact checked videos with a proxy related to the War in Ukraine - 704 • Number of videos removed as a result of a fact checking assessment with words related to the War in Ukraine - 133 • Number of videos not recommend in the For Your Feed as a result of a fact checking assessment with words related to the War in Ukraine - 124
<p>Collaborating with our fact-checking partners in relation to emerging trends (Commitment 31, Measure 31.1)</p>	<p>Description of intervention</p> <p>Since the beginning of the War in Ukraine, representatives from TikTok's misinformation policy and detection teams have met regularly with our external fact-checking partners, to receive advance warning of emerging misinformation narratives, facilitating proactive responses against high-harm trends.</p> <hr/> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p><i>Relevant metrics:</i></p> <ul style="list-style-type: none"> • Number of videos removed because of violation of misinformation policy with a proxy related to the War in Ukraine - 6,304

Reporting on the service's response during a crisis

Israel - Hamas Conflict

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

TikTok understands both the significance and sensitivity of the Israel-Hamas conflict (referred to as the "Conflict" throughout this section). Indeed, the Conflict, and commentary about it, illustrates the challenges inherent in successfully engaging in content moderation of violative content at scale while at the same time ensuring that the fundamental rights and freedoms of European citizens are respected and protected. We remain focused on supporting free expression, upholding our commitment to human rights, and maintaining the safety of our community and integrity of our platform during the Conflict. We

are also committed to transparency throughout this time and have kept our community informed of our immediate and ongoing response through the following Newsroom post: [Our continued actions to protect the TikTok community during the Israel-Hamas war](#).

Since the start of the Conflict on 7 October 2023, we have been working diligently to remove content that violates our policies. We have set out below some of the main threats both observed and considered in relation to the Conflict and the actions we have taken to address these.

(I) Spread of harmful misinformation

We believe that trust forms the foundation of our community, and we strive to keep TikTok a safe and authentic space where genuine interactions and content can thrive. TikTok takes a multi-faceted approach to tackling the spread of harmful misinformation, regardless of intent. This includes our: [Integrity & Authenticity policies \(I&A policies\)](#) in our [Community Guidelines \(CGs\)](#); as well as our external partnerships with fact-checkers, media literacy bodies, and researchers. We support our moderation teams with detailed misinformation policy guidance, enhanced training, and access to tools like our global database of previously fact-checked claims from our IFCN-accredited fact-checking partners, who help assess the accuracy of content.

Since 7 October 2023, there has been a rise in misinformation and conspiracy theories relating to the Conflict. We have also seen spikes in deceptive account behaviours and continue to take swift action against fake engagement and accounts, for example, by removing 35 million fake accounts in the month after the start of the Conflict - a 67% increase on the previous month.

(II) Covert Influence Operations (CIO)

TikTok's I&A policies do not allow deceptive behaviour that may cause harm to our community or society at large. This includes coordinated attempts to influence or sway public opinion while also misleading individuals, our community, or our systems about an account's identity, approximate location, relationships, popularity, or purpose. We have specifically-trained teams on high alert to investigate CIO and we provide quarterly updates on the CIO networks we detect and remove from our platform in our [Community Guidelines Enforcement Reports \(CGER\)](#).

We have assigned dedicated resourcing within our specialist teams to proactively monitor for CIO in connection with the Conflict. While we have not identified any CIO specifically targeting the Conflict during this reporting period, we reported on a CIO relevant to the region in our Q1 (Jan-March 2023) [CGER](#) where we identified and removed a network operated from Israel that targeted Israeli audiences. We are currently investigating a number of operations and will publish details of any CIO networks we identify and remove. While we currently report the removals of covert influence networks in the quarterly CGER, in the coming months, we will also introduce dedicated CIO reports to further increase transparency, accountability, and cross-industry sharing.

We know that CIO will continue to evolve in response to our detection and networks may attempt to re-establish a presence on our platform, which is why we continually seek to strengthen our policies and enforcement actions in order to protect our community against new types of harmful misinformation and inauthentic behaviours.

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



We are continually working hard to ensure that TikTok is a source of reliable and safe information and recognise the heightened risk and impact of misleading information during a time of crisis. As part of our crisis management process, we launched a command centre that brings together key members of our 40,000-strong global team of safety professionals, representing a range of expertise and regional perspectives, so that we remain agile in how we take action to respond to this fast-evolving crisis. Since the beginning of the Conflict, we are:

(I) Upholding TikTok's Community Guidelines

Continuing to enforce our [policies](#) against [violence](#), [hate](#), and [harmful misinformation](#) by taking action to remove violative content and accounts. For example, we remove content that promotes Hamas, or otherwise supports the attacks or mocks victims affected by the violence. If content is posted depicting a person who has been taken hostage, we will do everything we can to protect their dignity and remove content that breaks our rules. We do not tolerate attempts to incite violence or spread hateful ideologies. We have a zero-tolerance policy for content praising violent and hateful organisations and individuals, and those organisations and individuals aren't allowed on our platform. We also block hashtags that promote violence or otherwise break our rules.

Evolving our proactive automated detection systems in real-time as we identify new threats; this enables us to automatically detect and remove graphic and violent content so that neither our moderators nor our community members are exposed to it.

(II) Leveraging our Fact-Checking Program

We employ a layered approach to detecting harmful misinformation which is in violation of our Community Guidelines and our global fact-checking program is a critical part of this. The core objective of the fact-checking program is to leverage the expertise of external fact-checking organisations to help assess the accuracy of harmful and difficult to verify claims.

To limit the spread of potentially misleading information, we apply [warning labels](#) and prompt users to reconsider sharing content related to unfolding or emergency events, which have been assessed by our fact-checkers but cannot be verified as accurate i.e., 'unverified content'. Mindful about how evolving events may impact the assessment of sensitive Conflict related claims day-to-day, we have implemented a process that allows our fact-checking partners to update us quickly if claims previously assessed as 'unverified' become verified with additional context and/or at a later stage.

(III) Scaling up our content moderation capabilities

Since 7 October 2023, we have deployed additional Arabic and Hebrew speaking moderators in order to augment existing content moderation teams in reviewing content and assisting with Conflict-related translations. As we continue to focus on moderator care, we have also deployed additional well-being resources for our human moderation teams during this time.

(IV) Disruption of CIOs

Disrupting CIO networks has also been high priority work for us in tackling deceptive behaviour that may cause harm to our community or society at large. As noted above, although we have not identified any CIO that specifically targets the Conflict during this reporting period, we are investigating a number of



operations and will publish details of any CIO networks that we identify and remove in our CGER.

(V) Mitigating the risk of monetisation of harmful misinformation

Making temporary adjustments to policies that govern TikTok features in an effort to proactively prevent them from being used for hateful or violent behaviour in the region. For example, we've added additional restrictions on LIVE eligibility as a temporary measure given the heightened safety risk in the context of the current hostage situation. Our existing [political ads policy](#) and [safety and civility policies](#) help to mitigate the monetisation of harmful misinformation.

(VI) Deploying search interventions to raise awareness of potential misinformation

To help raise awareness and to protect our users, we have launched search interventions which are triggered when users search for non-violating terms related to the Conflict (e.g., Israel, Palestine). These search interventions remind users to pause and check their sources and also direct them to well-being resources.

(VII) Adding opt-in screens over content that could be shocking or graphic

We recognise that some content that may otherwise break our rules can be in the public interest, and we allow this content to remain on the platform for documentary, educational, and counterspeech purposes. Opt-in screens help prevent people from unexpectedly viewing shocking or graphic content as we continue to make [public interest exceptions](#) for some content.

In addition, we are committed to engagement with experts across the industry and civil society, such as [Tech Against Terrorism](#) and our [Advisory Councils](#), and cooperation with law enforcement agencies globally in line with our [Law Enforcement Guidelines](#), to further safeguard and secure our platform during these difficult times.

[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
I&A Policies	<p>We continue to rely on our existing, robust I&A policies, which are an effective basis for tackling content related to the Conflict. As such, we have not needed to introduce any new misinformation policies, for the purposes of addressing the crisis.</p> <p>In a crisis, we keep under review our policies and to ensure moderation teams have supplementary guidance.</p>	<p>In the context of the Conflict, we have been able to rely on our I&A policies, which are our first line of defence in combating harmful misinformation and deceptive behaviours on our platform.</p> <p>These guidelines make clear to our users what content we remove or make ineligible for the For You feed when they pose a risk of harm to our users or the wider public. We have also supported our moderation teams with detailed policy guidance and direction when moderating on Conflict-related harmful misinformation using existing policies.</p> <p>We have specialist teams within our Trust and Safety department dedicated to the policy issue of I&A, including within the areas of product and policy. Our experienced subject matter experts on I&A continually keep these policies under review and collaborate with external partners and experts when understanding whether updates are required.</p> <p>When situations such as the Conflict arise, these teams work to ensure that appropriate guidance is developed so that the I&A policies are applied in an effective manner in respect of content relating to the relevant crisis (in this case, the Conflict). This includes issuing detailed policy guidance and direction, including providing case banks on harmful misinformation claims to support moderation teams.</p>
TikTok Feature Policies	<p>In addition to being able to rely on our I&A policies, we have made temporary adjustments to existing policies which govern certain TikTok features. For example, we have added additional restrictions on LIVE eligibility as a temporary measure</p>	<p>Temporary adjustments have been introduced in an effort to proactively prevent certain features from being used for hateful or violent behaviour in the region.</p>



	<p>given the heightened safety risk in the context of the current hostage situation.</p>	
<p>Scrutiny of Ads Placements</p>		
<p>Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.</p>		
<p>Preventing misuse of our monetisation features (Commitment 1, Measure 1.1 and 1.4)</p>	<p>Description of intervention</p> <p>Our existing political ads policy and safety and civility policies help to mitigate the monetisation of harmful misinformation.</p> <p>We monitor the placement of our ads closely (especially in the context of events such as the Conflict) and in the event our ads are found to run adjacent to or on sources of disinformation, we will investigate to determine whether the content in question has been correctly identified and verify this with Integral Ad Science (IAS) or GARM as appropriate. We will then adjust any filters or add the publication in question to a blocklist to prevent a recurrence.</p> <p>NGOs that are vetted by Monetization Integrity and working with our sales team, are permitted to run ad campaigns for fundraising during the Conflict. This process operates with strict oversight to mitigate the risk of false fundraising campaigns. Also, in response to the Conflict, we have updated our LIVE feature guidelines to better prevent people from using monetisation features to exploit the ongoing tragedy for personal gain.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>Monitoring the placement of our ads and updating our LIVE policy helps to prevent people from monetising the ongoing tragedy for financial gain.</p>	
<p>Content moderation (Commitment 2, Measure 2.2)</p>	<p>Description of intervention</p> <p>We use a combination of automated and human moderation in order to identify content that breaches our ad policies. These policies prohibit, among other things, ad content and landing pages to display negative content regarding the military or police</p>	



	<p>symbols, sensitive military events, militarism, the advocating or whitewashing of war, terrorism, illegal organizations, or unlawful elements.</p> <p>We enforce our ad policies with a combination of automated and human moderation, and have expert teams focused on investigating and responding to any attempts to circumvent our policies.</p> <p>Our Monetisation Integrity department has moderation teams in multiple locations that speak Arabic and Hebrew.</p> <p><i>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</i></p> <p>Given the range of potential policy violations that could be engaged, we are currently unable to provide metrics specific to this issue.</p>
<p>Political Advertising</p>	
<p>Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.</p>	
<p>Prohibition on Political Advertising (Commitment 5, Measure 5.1)</p>	<p><i>Description of intervention</i></p> <p>In an effort to maintain both the integrity of the platform and safety of the people who use it, accounts belonging to politicians or political parties are not able to advertise or make money on TikTok.</p> <p>We do not allow paid political promotion, political advertising, or fundraising by politicians and political parties (for themselves or others). Our political ads policy includes both traditional paid ads and creators receiving compensation to support or oppose a candidate for office. This has been a long-standing policy at TikTok since 2019. We also do not allow ads and landing pages which:</p> <ul style="list-style-type: none"> ● reference, promote, or oppose candidates or nominees for public office, political parties, or elected or appointed government officials; ● reference an election, including voter registration, voter turnout, and appeals for votes; ● include advocacy for or against past, current, or proposed referenda, ballot measures, and legislative, judicial, or regulatory outcomes or processes (including those that promote or attack government policies or track records); and ● reference, promote, or sell, merchandise that features prohibited individuals, entities, or content, including campaign slogans, symbols, or logos.



	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>N/A</p>
<p>Integrity of Services</p>	
<p>Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.</p>	
<p>Identifying and removing CIO networks</p> <p><i>(Commitment 14, Measure 14.1)</i></p>	<p>Description of intervention</p> <p>We have assigned dedicated resourcing within our specialist teams to proactively monitor for CIO in connection with the Conflict.</p> <p>We fight against CIO as our I&A policies prohibit attempts to sway public opinion while also misleading our systems or users about the identity, origin, approximate location, popularity or overall purpose. We have specifically-trained and dedicated teams which are on high alert to investigate and detect CIO networks on our platform.</p> <p>We know that CIO will continue to evolve in response to our detection and networks may attempt to reestablish a presence on our platform, which is why we continually seek to strengthen our policies and enforcement actions in order to protect our community against new types of harmful misinformation and inauthentic behaviours.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>Although we have not identified any CIO that specifically targets the Conflict during this reporting period, we are investigating a number of operations and will publish details of any CIO networks that we do identify and remove within our CGER here.</p>
<p>Tackling synthetic and manipulated media</p> <p><i>(Commitment 15, Measures 15.1 and 15.2)</i></p>	<p>Description of intervention</p> <p>We do not allow synthetic media (AI-generated audio and visual content) content on the platform that may mislead our users or cause harm. Prohibited practices are set out in our I&A policies here.</p> <p>Our Synthetic and Manipulated Media Policy requires deceptive or synthetic media that shows realistic scenes must be clearly disclosed.</p>



	<p>On 19 September 2023, we launched a new AI-generated content label for creators to disclose content that is completely AI-generated or significantly edited by AI. For the purposes of our policy, synthetic media refers to content created or modified by AI technology. It includes highly realistic digitally-created (fake) content of real people, such as a video of a real person speaking but their words have been modified or changed.</p>
	<p><i>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</i></p> <p>Our efforts support transparent and responsible content creation practices, both in the context of the Conflict and more broadly on our platform.</p>
<p>Removing harmful misinformation from our platform (Commitment 14, Measure 14.1)</p>	<p><i>Description of intervention</i></p> <p>We take action to remove accounts or content which contain inaccurate, misleading, or false information that may cause significant harm to individuals or society, regardless of intent. In conflict environments, such information may include content that is repurposed from past conflicts, content which makes false and harmful claims about specific events, or incites panic. In certain circumstances, we may also reduce the prominence of such content.</p> <p>We employ a layered approach to misinformation detection, leveraging multiple overlapping strategies to ensure comprehensive and responsive coverage. We place considerable emphasis on proactive content moderation strategies in order to remove harmful misinformation which is in violation of our policies before it is reported to us by users or third parties.</p> <p><i>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</i></p> <p>In the context of the Conflict, we are proud to have proactively removed over 30,000 videos containing harmful misinformation related to the Conflict. We have been able to do this through a combination of automation and human moderation, carrying out targeted sweeps of certain types of content (e.g. hashtags/sensitive keyword lists) as well as working closely with our fact-checking partners and responding to emerging trends they identify.</p> <p>We have scaled up our Arabic and Hebrew speaking content moderation as we recognise the importance of language and cultural context in the misinformation moderation process.</p> <p><i>Relevant metrics:</i></p> <ul style="list-style-type: none"> ● Number of videos removed because of violation of misinformation policy with a proxy (IL/Hamas) - 33,392 ● Number of videos not recommended because of violation of misinformation policy with a proxy (IL/Hamas) - 43,658 ● Number of proactive removals of videos removed because of violation of misinformation policy with a proxy IL/Hamas 30,312

Empowering Users

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

Deploying search interventions to raise awareness of potential misinformation

(Commitment 21, Measure 21.1)

Description of intervention

To minimise the discoverability of misinformation and help to protect our users, we have launched search interventions which are triggered when users search for neutral terms related to the Conflict (e.g., Israel, Palestine).

Indication of impact (at beginning of action: expected impact) including relevant metrics when available

These search interventions remind users to pause and check their sources and also direct them to well-being resources.

Not proactively promoting news-type content to our users

(Commitment 18, Measure 18.1)

Description of intervention

TikTok is primarily an entertainment platform. It may be the case that a user's For You feed shows more news-type content (such as news content relating to the Conflict) over time if that is content that a user is actively looking for and engaging with, but we do not actively promote news content to users on TikTok.

Further, TikTok's recommender system delivers a personalised feed of content based on a user's engagement behaviour with video content types. Every user's feed will look different, according to their own preferences, which are demonstrated through 'likes', watch duration and other related metrics. For more information on how our recommendation system works, see [here](#).

Indication of impact (at beginning of action: expected impact) including relevant metrics when available

Our approach to news-type content supports our efforts to reduce the spread of harmful disinformation to users.

Empowering the Research Community

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



<p>Measures taken to support research into Conflict- related misinformation and disinformation</p> <p><i>(Commitment 26, Measure 26.1 and 26.2)</i></p>	<p>Description of intervention</p> <p>Through our Research API, academic researchers from non-profit universities in the US and Europe can apply to study public data about TikTok content and accounts. This public data includes comments, captions, subtitles, and number of comments, shares, likes, and favourites that a video receives. More information is available here.</p> <hr/> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>Since 7 October 2023, 5 Research API applications related to the Conflict have been approved.</p>
<p>Empowering the Fact-Checking Community</p>	
<p>Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.</p>	
<p>Applying our unverified content label to make content ineligible for recommendation</p> <p><i>(Commitment 31, Measure 31.2)</i></p>	<p>Description of intervention</p> <p>Where our misinformation moderators or fact-checking partners determine that content is not able to be verified at the given time (which is common during an emergency or unfolding event), we apply our unverified content label to the content to encourage users to consider the reliability or source of the content. The application of the label will also result in the content becoming ineligible for recommendation in order to limit the spread of potentially misleading information</p> <hr/> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>Verifying certain information during dynamic and fast moving events such as the Conflict can be challenging and our moderators and fact-checkers cannot always conclusively determine whether content is indeed harmful misinformation. Therefore, in order to minimise risk, where our fact-checkers or our moderators do not have enough information to verify content which may potentially be misleading, we apply our unverified content label to inform users the content has been reviewed but cannot be conclusively validated. The goal is to raise users' awareness about the credibility of the content and to reduce sharing (see screenshots here). Our unverified content label is available to users in 23 EU official languages (plus, for EEA users, Norwegian and Icelandic).</p> <p>Where the banner is applied, the content will also become ineligible for recommendation into anyone's For You feed to limit the spread of information relating to unfolding events where details are still developing and which may potentially be misleading.</p>



<p>Ensuring fact-checking coverage</p> <p><i>(Commitment 30, Measure 30.1)</i></p>	<p>Description of intervention</p> <p>As part of our fact-checking program, TikTok works with 18 IFCN-accredited fact-checking organisations that support more than 50 languages, including Hebrew and Arabic, to help assess the accuracy of content in this rapidly-changing environment. In the context of the Conflict, our independent fact-checking partners are following our standard practice, whereby they do not moderate content directly on TikTok, but assess whether a claim is true, false, or unsubstantiated so that our moderators can take action based on our CGs. Fact-checker input is then incorporated into our broader content moderation efforts in a number of different ways, as further outlined in the ‘indication of impact’ section below.</p> <p>In the context of the Conflict, we have also adjusted our information consolidation process to allow us to track and store Conflict related claims separately from our global repository of previously fact-checked claims. This facilitates quick and effective access to relevant assessments, which, in turn, increases the effectiveness of our moderation efforts.</p> <hr/> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>We see harmful misinformation as different from other content issues. Context and fact-checking are critical to consistently and accurately enforcing our harmful misinformation policies, which is why we have ensured that, in the context of the crisis, our fact-checking programme covers Arabic and Hebrew.</p> <p>As noted above, we also incorporate fact-checker input into our broader content moderation efforts in different ways:</p> <ul style="list-style-type: none"> • Proactive insight reports that flag new and evolving claims they’re seeing across the internet. This helps us detect harmful misinformation and anticipate misinformation trends on our platform. • Collaborating with our fact-checking partners to receive advance warning of emerging misinformation narratives has facilitated proactive responses against high-harm trends and has helped to ensure that our moderation teams have up-to-date guidance. • A repository of previously fact-checked claims to help misinformation moderators make swift and accurate decisions. <p><i>Relevant metrics:</i></p> <ul style="list-style-type: none"> • Number of fact checked tasks related to IL/Hamas - 2,672 • Number of videos removed as a result of a fact checking assessment with words related to IL/Hamas - 532 • Number of videos demoted (NR) as a result of a fact checking assessment with words related to IL/Hamas - 588
---	--



<p>Collaborating with our fact-checking partners in relation to emerging trends</p> <p><i>(Commitment 31, Measure 31.1)</i></p>	<p>Description of intervention</p> <p>Since the beginning of the Conflict, representatives from TikTok's misinformation policy and product teams have connected regularly with our external fact-checking partners, to receive advance insights into emerging misinformation narratives, facilitating proactive responses against high-harm trends.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p><i>Relevant metrics:</i></p> <ul style="list-style-type: none"> • Number of videos removed because of violation of misinformation policy with a proxy (IL/Hamas) - 33,392



Reporting on the service’s response during an election

European Elections

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

As co-chair of the Code of Practice on Disinformation's Working Group on elections, TikTok takes our role of [protecting the integrity of elections](#) on our platform very seriously. We have comprehensive measures in place to anticipate and address the risks associated with electoral processes, including the risks associated with election misinformation in the context of the **Elections** for the **European Parliament** that will take place in June 2024 (“EU Elections”). We recognise both the significance and scale of the forthcoming EU Elections, in which many of the 142m people from across the 27 EU Member States who come to TikTok every month, will vote to decide their political direction.

In terms of threats in relation to the EU Elections, we anticipate increased risks to come from both user generated content (UGC) and **AI-generated content (AIGC)**. With AIGC, there is an increased risk of, for example, disinformation campaigns, efforts to discredit politicians, and the proliferation of fake political endorsements by celebrities, targeting younger voters. Cognizant of these risks, TikTok is pleased to have joined industry partners in pledging to [Combat Deceptive Use of AI in 2024 Elections](#). Whilst this is a recent initiative, we look forward to sharing information on our related efforts in future reports. Separately, we also anticipate potential risks of **Covert Influence Operations (CIO)** and **Impersonation** targeting parties, politicians and endorsers.

With these risks in mind, we will establish a dedicated 'Mission Control' space in our Dublin office bringing together our key personnel from the different teams involved in the election monitoring process. The centralised space for the EU Elections will allow fast and clear communication on topics that may arise during an election period and maximise the effectiveness of our election integrity work.

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

In addition to the dedicated Mission Control space described above, we have a comprehensive strategy to ensure that TikTok remains a creative, safe, and civil place for our community during the election period. This will be achieved through a combination of enforcing our policies, directing people to trusted information and engaging with external stakeholders and national and EU authorities and political bodies.

Enforcing our policies**(I) Moderation capabilities**

We have over 6,000 people dedicated to moderating EU language content. Our teams work alongside technology to ensure that we are consistently [enforcing our rules](#) to detect and remove misinformation, CIOs, and other content and behaviour that can increase during an election period.

(II) Countering misinformation

In Q3 2023, 99% of all the content we removed for election and civic misinformation was taken down before it was reported to us. Our misinformation moderators receive enhanced training and tools to detect and remove misinformation and other violative content. We also have teams on the ground who partner with experts to ensure local context and nuance is reflected in our approach.

(III) Fact-checking

We employ a layered approach to detecting harmful misinformation which is in violation of our CGs and our global fact-checking program is a critical part of this. The core objective of the fact-checking program is to leverage the expertise of external fact-checking organisations to help assess the accuracy of harmful and difficult to verify claims.

We work with 11 [independent fact-checking organisations](#) in Europe, who assess the accuracy of content in 18 different European languages, and we [label any claims that cannot be verified](#). Ahead of the EU Elections, we are planning to cover at least one official language of each of the European Member States and will be expanding our misinformation moderation teams' coverage accordingly.

(IV) Deterring covert influence operations

Deceptive actors do sometimes try to target online platforms during elections, and we have dedicated experts working to detect, disrupt, and stay ahead of deceptive behaviours. We report the removals of covert influence networks in our quarterly [Community Guidelines Enforcement Reports](#). In the coming months, we'll also introduce dedicated covert influence operations reports to further increase transparency, accountability, and cross-industry sharing. We currently provide information about how we assess this behaviour on our [Transparency Center](#).

(V) Tackling misleading AI-generated content

AIGC brings new challenges around misinformation, which we've proactively addressed with firm [rules](#) and new [technologies](#). We do not allow manipulated content that could be misleading, including AIGC of public figures if it depicts them endorsing a political view. We also require creators to label any realistic AIGC and in September 2023, we launched a first-of-its-kind [AI-generated content label](#) to help people do this. TikTok is one of 20 industry partners pledging to [Combat Deceptive Use of AI in 2024 Elections](#). This builds on our continued investment in protecting election integrity and advancing responsible and transparent AIGC practices through robust rules, new technologies, and media literacy partnerships with experts. As the technology evolves, we will continue to strengthen our efforts, including by working with industry through content provenance partnerships.

(VI) Government, Politician, and Political Party Accounts (GPPAs)

Many European leaders, ministers, and political parties are joining the platform, including approx. 30% of Members of European Parliament (**MEPs**) and the EU Parliament itself. These politicians and parties play an important role on our platform - we believe that verified accounts belonging to politicians and institutions provide the electorate with another route to access their representatives, and additional trusted voices in the shared fight against misinformation. In the lead up to the EU Elections, we are taking steps to engage with both sitting MEPs and candidates from across the 27 EU Member States to ensure they have the necessary information to use TikTok safely and authentically, and can get their accounts verified, should they wish to join the platform.

We strongly recommend [GPPAs get verified](#). Verified badges help users make informed choices about the accounts they choose to follow. It's also an easy way for notable figures to let users know they're seeing authentic content, and it helps to build trust among high-profile accounts and their followers. For individuals, non-profits, institutions, businesses, or official brand pages, this badge builds an important layer of clarity with the TikTok community.

Directing people to trusted sources

(I) EU 27 In-app Election Centers

TikTok will launch localised in-app Election Centres for each of the individual 27 EU Member States to ensure people can easily separate fact from fiction. Working with local electoral commissions and civil society organisations, these Election Centres will be a place where our community can find trusted and authoritative information.

(II) Investing in media literacy

We invest in media literacy campaigns as a counter-misinformation strategy. In 2023, we collaborated with fact checkers to launch media literacy campaigns in many EU countries generating over 220m impressions and reaching approx. 50m people on TikTok. This work will continue this year with localised media literacy activations in all 27 EU Member States ahead of the EU Elections in June 2024.

External engagement at the national and EU levels



(I) Engagement with local experts

To further promote election integrity, and inform our approach to the upcoming EU Elections, our Election Speaker Series will see local and regional external experts, particularly from the fact-checking community, invited to share their insights and market expertise with our internal teams.

(II) Engagement with national authorities and stakeholders

In order to prepare for the upcoming EU Elections, our Government Relations teams have been engaging with relevant authorities in many EU Member States.

For instance, in Sweden, since H2 2023, we have conducted meetings and consultations at the national level with local experts, parliamentary parties and other party representatives, and the Swedish Election Authority on election integrity and data security in advance of the upcoming EU Elections.

We will continue meeting with national agencies and stakeholders in the coming weeks.

(III) Engagement at the EU-level

Engagement with the European Parliament and EU political parties

Our teams have also been closely engaging with the European Parliament since mid-2023 in order to discuss our preparations for the EU Elections and answer questions about our policies.

We participated in the Social Media Conference organised by the European Parliament's communications team in November 2023 to present our approach to election integrity and our rules for political account holders.

Our teams continue to actively engage with European political groups and political parties, to explain our approach to elections, and answer their questions about our policies.

Engagement with the EU authorities

In the context of national EU elections, such as the Slovakian parliamentary elections in September 2023 and the Polish parliamentary election in October 2023, our teams have also been in contact with the EU Commission to share insights and describe our approach to election preparedness across the EU. Similarly, ahead of the upcoming EU Elections, our teams are engaging with the EU Commission, including regarding the proposed draft Digital Services Act (**DSA**) guidelines on the integrity of electoral processes.



[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
Integrity and Authenticity (I&A) Policies	<p>We continue to rely on our existing, robust I&A policies and as such have not needed to introduce new policies in advance of the EU Elections.</p>	<p>We have been able to rely on the I&A policies in our CGs, which are our first line of defence in combating misinformation, civic and election integrity, and deceptive behaviours on our platform. Our CGs make clear to our users what content we remove or make ineligible for the For You feed when they pose a risk of harm to our users or the wider public.</p> <p>We have over 6,000 people dedicated to moderating EU language content. Our teams work alongside technology to ensure that we are consistently enforcing our rules to detect and remove misinformation, covert influence operations, and other content and behaviour that can increase during an election period. We will also support our moderation teams with detailed policy guidance and direction when moderating on EU Elections related content.</p> <p>We have specialist teams within our Trust and Safety department dedicated to the policy issue of I&A, including within the areas of product and policy. Our experienced subject matter experts on I&A continually keep these policies under review and collaborate with external partners and experts when understanding whether updates are required.</p> <p>In the lead-up to the EU Elections, these teams work to ensure that appropriate guidance is developed so that the I&A policies are applied in an effective manner.</p> <p><i>Enforcement of our I&A policies in relation to GPPAs</i></p>



		<p>Accounts belonging to GPPPA and news organisations play a unique role in civic discourse, and while we remove their violative content like we do for anyone else, we also apply more nuanced account enforcement policies to protect the public interest. For example, if such an account were to post content promoting misinformation that could undermine a civic process or contribute to real-world harm during an election period, we may restrict that account from posting content for up to 30 days, in addition to removing the content for breaking our rules.</p>
<p>Scrutiny of Ads Placements</p>		
<p>Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.</p>		
<p>Ban on monetisation features and fundraising campaigns for GPPPAs (Commitment 7 and Measure 7.1)</p>	<p><i>Description of intervention</i></p> <p>We classify relevant political TikTok accounts as a Government, Politician, and Political Party Account (GPPPA). GPPPAs can include government-run entities, elected officials or candidates, political parties, current/former heads of state or government. Where accounts are designated as GPPPAs, they are banned from placing ads (see “Political Advertising” section) on TikTok and from monetisation features.</p> <p>Solicitations for campaign fundraising by GPPPAs are not permitted either on the platform. That includes content like a video from a politician asking for donations, or a political party directing people to a donation page on their website. We provide GPPPAs account holders with information on our policies and moderation systems as well as actively encourage them to verify their profiles. Read more here.</p> <p>In order to enforce these policies, our local Government Relations teams ensure that as many EU GPPPAs accounts as possible are identified and labelled correctly ahead of the EU Elections.</p> <hr/> <p><i>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</i></p> <p>Our GPPPA-specific policies help us recognise the public interest associated with these accounts, while also putting guardrails in place (for example by restricting advertising and monetisation features).</p>	



	Political Advertising
--	------------------------------

<p>Prohibition on Political Advertising (Commitment 5, Measure 5.1)</p>	<p>TikTok does not allow political advertising on the platform.</p> <p>We recognise that some members of our community may want to create or engage with political content on TikTok and so sharing political beliefs and engaging in political conversation is allowed as organic content provided it does not violate our CGs. However, users cannot pay to advertise or promote this content. Furthermore, in an effort to maintain both the integrity of the platform and safety of the people who use it, accounts belonging to politicians or political parties cannot advertise or make money on TikTok.</p> <p>We do not allow paid political promotion, political advertising, or fundraising by politicians and political parties (for themselves or others). Our political ads policy includes both traditional paid ads and creators being paid to make branded political content. This has been a long-standing policy at TikTok since 2019. We don't allow paid or branded content that promotes or opposes a candidate, current leader, political party or group, or issue at the federal, state, or local level – including election-related ads, advocacy ads, or issue ads. This means that accounts we identify as belonging to politicians and political parties have their access to advertising features turned off.</p> <p>All ads are reviewed before being displayed on our platform. Upon review, if an ad is deemed to violate our ad policies including our prohibition of political ads, it will not be permitted on our platform. We also review ads reported to us and upon review, violating ads will be removed. Our community can also report ads that they believe break our rules, which our teams will review and remove if they are found to be violative.</p> <p>During the EU Elections, we will increase our risk mitigation measures for political content due to the risk of increased political activity on the platform through:</p> <ul style="list-style-type: none"> ● monitoring for EU politicians ● monitoring for EU political parties ● monitoring for EU disinformation trends <p>TikTok also works with local politicians to ensure that they are correctly onboarded onto the platform and are aware of TikTok's political advertising policy.</p>
--	---



	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>By prohibiting political advertising, we help ensure our community can have a creative and authentic TikTok experience, and we reduce the risk of our platform being used to advertise and amplify narratives that may be divisive or false.</p>
<p>Integrity of Services</p>	
<p>Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.</p>	
<p>Identifying and removing CIO networks</p> <p><i>(Commitment 14, Measure 14.1)</i></p>	<p>Description of intervention</p> <p>In advance of the EU Elections in June 2024, we will establish a dedicated 'Mission Control' space in our Dublin office, home to our EMEA Trust & Safety Hub. This will bring together our specialist elections team, including members of our team in charge of disrupting covert influence operations (CIO), to maximise the effectiveness of our work in the run-up to, and during, the elections.</p> <p>We have dedicated resourcing assigned to monitor for threats during the EU Elections period.</p> <p>While we have, in the past, disrupted CIO targeting discourse around a particular European election, more commonly we have disrupted CIOs targeting EU Member States with more broad and holistic strategic discourse. This is documented in our quarterly Community Guidelines Enforcement Reports, which includes information on the CIOs we identify and disrupt during each reporting period.</p> <p>Based on our transparency reporting up until Q3 2023, 11 CIOs were assessed to have targeted EU Member States with broader narratives and 1 CIO was assessed to have targeted an EU Member State with election specific narratives. We expect to see similar trends throughout the EU Election period, and we are primed to respond appropriately.</p> <p>To date, we have not detected any CIOs solely focussed on the EU Elections. We will proactively monitor for EU Election specific content should it be uncovered as either part of wider covert influence narratives in upcoming investigations as we draw closer to the election, or as emerging covert influence attempts specifically targeting EU elections discourse.</p>



	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>The proactive monitoring for EU Election specific content by our experienced and trained teams should allow us to detect and disrupt CIOs targeting the EU in the context of the EU Elections in a timely manner.</p>
<p>Tackling synthetic media</p> <p><i>(Commitment 15, Measures 15.1 and 15.2)</i></p>	<p>Description of intervention</p> <p>We do not allow synthetic media (AI-generated audio and visual content) content on the platform that may mislead our users or cause harm.</p> <p>Our Synthetic and Manipulated Media Policy makes it clear that we do not want our users to be misled about political issues. Thus, synthetic media about public figures, such as politicians, must be clearly labelled as AI generated, and can not be used for political and commercial endorsements. For the purposes of our policy, synthetic media refers to content created or modified by AI technology. It includes highly realistic digitally-created (fake) content of real people, such as a video of a real person speaking but their words have been modified or changed.</p> <p>In September 2023, we launched a new AI-generated content label for creators to easily inform their community when they post AI-generated content. The label can be applied to any content that has been completely generated or significantly edited by AI which makes it easier to comply with the obligation to disclose AI-generated content that shows realistic scenes. Creators can do this through this label or through other types of disclosures, like a sticker or caption.</p> <p>Lastly, acknowledging that it is crucial for tech companies to work together to safeguard communities against misleading and deceptive AI in this historic election year, TikTok has joined industry partners as a party to the Tech Accord to Combat Deceptive Use of AI in 2024 Elections. Through this Accord, we pledged to work collaboratively on tools to detect and address online distribution of such AI content and acknowledge the importance of tracking the origin of deceptive election-related content and the need to raise public awareness about the problem.</p> <p>Our efforts support transparent and responsible content creation practices, both in the context of the EU Elections and more broadly on our platform.</p>
<p>Empowering Users</p>	
<p>Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.</p>	



<p>Rolling out Media literacy campaigns (<i>Commitment 17, Measure 17.2</i>)</p>	<p>Description of intervention</p> <p>In preparation for the EU Elections, we will launch localised in-app Election Centres for each of the individual 27 EU Member States. We want to empower users with trusted and authoritative information to help them distinguish fact from fiction and reduce the effectiveness of any attempts at disseminating election-related misinformation. Users will be directed to a bespoke, language-specific in-app Election Center through a variety of entry points, e.g., when they search election content, video notice tags, banners displayed on Live content, or Push notifications.</p> <p>On the Election Centers, our users will receive information about the EU Elections and EU institutions, “how to vote”, media literacy content, and an election day countdown. They will also be signposted to non-partisan third party bodies such as national election commissions, civil society organisations and the European Parliament for authoritative and trusted sources of information. To further promote election integrity and tackle election misinformation, we are working toward localised media literacy activations in all 27 EU Member States by the end of 2024 with the majority being activated ahead of the EU Elections.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>27 in-app EU Election Centers.</p> <p>Providing a proactive tool to all our EU users and equipping them with authoritative information in their local languages will help to reduce the effectiveness of campaigns and efforts at disseminating election-related misinformation. Our Election Centers will also provide a greater visibility to the resources made available by authoritative and trusted sources on the occasion of the EU Elections.</p>
<p>Engagement with local and regional experts (<i>Commitment 17, Measure 17.2</i>)</p>	<p>Description of intervention</p> <p>Our internal teams will also benefit from the insights and market expertise shared by the external experts from various EU Member States, particularly from the fact-checking community, we invite as part of our ongoing Election Speaker Series.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>This engagement with external experts allows us to inform our country-level approaches because, although the EU elections represent a unique transnational democratic process, in practice, these elections will consist of 27 national elections.</p>



Empowering the Research Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
<p>Providing access to our Research API (Commitment 26 and Measures 26.1 and 26.2)</p>	<p>Description of intervention</p> <p>Through our Research API, academic researchers from non-profit universities in the US and Europe can apply to study public data about TikTok content and accounts. This public data includes comments, captions, subtitles, and number of comments, shares, likes, and favourites that a video receives, comments from our platform. More information is available here.</p> <p>In advance of the upcoming EU Parliamentary elections in June 2024, we have approved 4 Research API applications from the EU (2 from Germany, Netherlands, and Portugal) and 1 from the UK with EU Elections specific research topics that include: detecting CIO, deep fakes, content published by running candidates and parties, and the origin and impact of false narratives debunked by fact-checkers.</p> <p>Additionally, 5 research applications from the EEA (Denmark, Germany, Netherlands and 2 from Norway) have been approved in relation to EU local elections (Germany, Netherlands, Denmark, Sweden).</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>4 Research API applications related to the EU Elections have been approved.</p>
Empowering the Fact-Checking Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
<p>Ensuring fact-checking coverage (Commitment 30, Measure 30.1)</p>	<p>Description of intervention</p> <p>Our teams will be ensuring fact-checking coverage by a combination of permanent and temporary partnerships covering at least one official language of each of the European Member States ahead of the EU Elections. We will be expanding our misinformation moderation teams' coverage accordingly.</p>



	<p><i>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</i></p> <p>Before the EU Election, we will have fact-checking coverage in at least one official language of each of the European Member States</p>
<p>Ensuring fact-checker’s access to relevant information (Commitment 32, Measure 32.3)</p>	<p><i>Description of intervention</i></p> <p>In September 2023, we held a 2-day roundtable discussion with a number of our fact-checking partners across the EMEA region. The purpose of the discussion was to provide our fact-checking partners with information about our procedures - in particular, our end-to-end moderation process (of which they form an integral part), I&A policy development, and Community Guidelines enforcements. As part of this roundtable, we held a dedicated session on collaboration around the EU Elections and discussed the possibility of enhanced fact-checking coverage, e.g., weekend coverage).</p> <p>As part of our EU Elections preparedness efforts, and throughout the process and outcome, we will remain in regular contact with our fact-checking partners to ensure we are keeping people safe and protecting the integrity of the TikTok platform.</p>
	<p><i>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</i></p> <p>Our dedicated fact-checking program is an integral part of our strategy to detect and mitigate the spread of misinformation during the EU Elections. Regular contact with our European fact-checkers fosters cooperation and readiness for the EU Elections.</p>