

Code of Practice on Disinformation – Report of TikTok for the period 1 January 2025 - 31 June 2025



Table of Contents

Executive summary.....	13
II. Scrutiny of Ad Placements.....	19
Commitment 1.....	20
Measure 1.1.....	21
Measure 1.2.....	21
Measure 1.3.....	22
Measure 1.4.....	24
Measure 1.5.....	24
Measure 1.6.....	24
Commitment 2.....	24
Measure 2.1.....	26
Measure 2.2.....	28
Measure 2.3.....	29
Measure 2.4.....	32
Commitment 3.....	35
Measure 3.1.....	36
Measure 3.2.....	36
Measure 3.3.....	37
III. Political Advertising.....	38
Commitment 4.....	39
Measure 4.1.....	39
Measure 4.2.....	39
Commitment 5.....	40
Measure 5.1.....	40
Commitment 6.....	41
Measure 6.1.....	41
Measure 6.2.....	41
Measure 6.3.....	42
Measure 6.4.....	42
Measure 6.5.....	42
Commitment 7.....	43
Measure 7.1.....	43
Measure 7.2.....	44
Measure 7.3.....	44
Measure 7.4.....	44
Commitment 8.....	45
Measure 8.1.....	45
Measure 8.2.....	45
Commitment 9.....	46
Measure 9.1.....	46
Measure 9.2.....	46
Commitment 10.....	47



Measure 10.1.....	47
Measure 10.2.....	47
Commitment 11.....	48
Measure 11.1.....	48
Measure 11.2.....	48
Measure 11.3.....	48
Measure 11.4.....	48
Commitment 12.....	49
Measure 12.1.....	49
Measure 12.2.....	49
Measure 12.3.....	50
Commitment 13.....	50
Measure 13.1.....	50
Measure 13.2.....	50
Measure 13.3.....	51
IV. Integrity of Services.....	52
Commitment 14.....	53
Measure 14.1.....	55
Measure 14.2.....	64
Measure 14.3.....	117
Commitment 15.....	118
Measure 15.1.....	120
Measure 15.2.....	122
Commitment 16.....	122
Measure 16.1.....	123
Measure 16.2.....	125
V. Empowering Users.....	126
Commitment 17.....	127
Measure 17.1.....	133
Measure 17.2.....	163
Measure 17.3.....	199
Commitment 18.....	202
Measure 18.1.....	204
Measure 18.2.....	205
Measure 18.3.....	213
Commitment 19.....	214
Measure 19.1.....	215
Measure 19.2.....	218
Commitment 20.....	221
Measure 20.1.....	221
Measure 20.2.....	222
Commitment 21.....	222
Measure 21.1.....	225
Measure 21.2.....	236



Measure 21.3.....	236
Commitment 22.....	236
Measure 22.1.....	237
Measure 22.2.....	238
Measure 22.3.....	238
Measure 22.4.....	238
Measure 22.5.....	238
Measure 22.6.....	239
Measure 22.7.....	239
Commitment 23.....	241
Measure 23.1.....	241
Measure 23.2.....	245
Commitment 24.....	247
Measure 24.1.....	248
Commitment 25.....	256
Measure 25.1.....	256
Measure 25.2.....	257
VI. Empowering the research community.....	258
Commitment 26.....	259
Measure 26.1.....	260
Measure 26.2.....	262
Measure 26.3.....	267
Commitment 27.....	267
Measure 27.1.....	268
Measure 27.2.....	268
Measure 27.3.....	268
Measure 27.4.....	269
Commitment 28.....	269
Measure 28.1.....	270
Measure 28.2.....	274
Measure 28.3.....	275
Measure 28.4.....	275
Commitment 29.....	275
Measure 29.1.....	276
Measure 29.2.....	277
Measure 29.3.....	277
VII. Empowering the fact-checking community.....	278
Commitment 30.....	279
Measure 30.1.....	280
Measure 30.2.....	289
Measure 30.3.....	290
Measure 30.4.....	290
Commitment 31.....	290
Measure 31.1.....	291



Measure 31.2.....	292
Measure 31.3.....	299
Measure 31.4.....	300
Commitment 32.....	300
Measure 32.1.....	301
Measure 32.2.....	301
Measure 32.3.....	301
Commitment 33.....	302
Measure 33.1.....	302
VIII. Transparency Centre.....	304
Commitment 34.....	305
Measure 34.1.....	305
Measure 34.2.....	305
Measure 34.3.....	306
Measure 34.4.....	306
Measure 34.5.....	306
Commitment 35.....	306
Measure 35.1.....	307
Measure 35.2.....	307
Measure 35.3.....	307
Measure 35.4.....	307
Measure 35.5.....	307
Measure 35.6.....	307
Commitment 36.....	307
Measure 36.1.....	308
Measure 36.2.....	308
Measure 36.3.....	308
IX. Permanent Task-Force.....	309
Commitment 37.....	310
Measure 37.1.....	310
Measure 37.2.....	310
Measure 37.3.....	310
Measure 37.4.....	311
Measure 37.5.....	311
Measure 37.6.....	311
X. Monitoring of Code.....	312
Commitment 38.....	313
Measure 38.1.....	313
Commitment 39.....	314
Commitment 40.....	315
Measure 40.1.....	315
Measure 40.2.....	316
Measure 40.3.....	316
Measure 40.4.....	316



Measure 40.5.....	316
Measure 40.6.....	316
Commitment 41.....	316
Measure 41.1.....	317
Measure 41.2.....	317
Measure 41.3.....	317
Commitment 42.....	318
Commitment 43.....	318
War of aggression by Russia on Ukraine.....	320
Israel - Hamas Conflict.....	335
Polish Election 2025.....	350
German Federal Election 2025.....	360
Portuguese Election 2025.....	371
2025 Romanian Presidential Election.....	381

Commitments	Measures	Service A
II. Scrutiny of Ad Placements		
1	Measure 1.1	<input type="checkbox"/>
	Measure 1.2	<input type="checkbox"/>
	Measure 1.3	<input checked="" type="checkbox"/>
	Measure 1.4	<input type="checkbox"/>
	Measure 1.5	<input type="checkbox"/>
	Measure 1.6	<input 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 type="checkbox"/>
	Measure 4.2	<input type="checkbox"/>
5	Measure 5.1	<input type="checkbox"/>
6	Measure 6.1	<input type="checkbox"/>
	Measure 6.2	<input type="checkbox"/>
	Measure 6.3	<input type="checkbox"/>
	Measure 6.4	<input type="checkbox"/>
	Measure 6.5	<input type="checkbox"/>
7	Measure 7.1	<input type="checkbox"/>
	Measure 7.2	<input type="checkbox"/>
	Measure 7.3	<input type="checkbox"/>
	Measure 7.4	<input type="checkbox"/>
8	Measure 8.1	<input type="checkbox"/>



	Measure 8.2	<input type="checkbox"/>
9	Measure 9.1	<input type="checkbox"/>
	Measure 9.2	<input type="checkbox"/>
10	Measure 10.1	<input type="checkbox"/>
	Measure 10.2	<input type="checkbox"/>
11	Measure 11.1	<input type="checkbox"/>
	Measure 11.2	<input type="checkbox"/>
	Measure 11.3	<input type="checkbox"/>
	Measure 11.4	<input 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 type="checkbox"/>
	Measure 13.2	<input type="checkbox"/>
	Measure 13.3	<input 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 type="checkbox"/>
	Measure 18.2	<input checked="" type="checkbox"/>
	Measure 18.3	<input 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 type="checkbox"/>
	Measure 21.3	<input 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 type="checkbox"/>
	Measure 27.2	<input type="checkbox"/>
	Measure 27.3	<input type="checkbox"/>
	Measure 27.4	<input 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 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 type="checkbox"/>
	Measure 31.2	<input checked="" type="checkbox"/>
	Measure 31.3	<input type="checkbox"/>
	Measure 31.4	<input 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	☒
36	Measure 36.1	☒
	Measure 36.2	☒
	Measure 36.3	☒
IX. Permanent Task-Force		
37	Measure 37.1	☒
	Measure 37.2	☒
	Measure 37.3	☒
	Measure 37.4	☒
	Measure 37.5	☒
	Measure 37.6	☒
X. Monitoring of the Code		
38	Measure 38.1	☒
39	-	☐
40	Measure 40.1	☒
	Measure 40.2	☒
	Measure 40.3	☒
	Measure 40.4	☒
	Measure 40.5	☒
	Measure 40.6	☒
41	Measure 41.1	☒
	Measure 41.2	☒
	Measure 41.3	☒
42	-	☒
43	-	☒



Executive summary

About TikTok

TikTok's mission is to inspire creativity and bring joy. With a global community of more than a billion users, it's natural for people to hold different opinions. That's why we focus on a shared set of facts when it comes to issues that affect people's safety. A safe, authentic, and trustworthy experience is essential to achieving our goals. Transparency plays a key role in building that trust, allowing online communities and society to assess how TikTok meets its regulatory obligations. As a signatory to the Code of Conduct on Disinformation (the Code), TikTok is committed to sharing clear insights into the actions we take.

TikTok takes disinformation extremely seriously. We are committed to preventing its spread, promoting authoritative information, and supporting media literacy initiatives that strengthen community resilience.

We prioritise proactive content moderation, with the vast majority of violative content removed before it is viewed or reported. In H1 2025, more than 97% of videos violating our Integrity and Authenticity policies were removed proactively worldwide.

We continue to address emerging behaviours and risks through our Digital Services Act (DSA) compliance programme, which the Code has operated under since July 2025. This includes a range of measures to protect users, detailed on our [European Online Safety Hub](#).

Our actions under the Code demonstrate TikTok's strong commitment to combating disinformation while ensuring transparency and accountability to our community and regulators.

Our sixth report under the Code - 1 January to 31 June 2025

TikTok has been an active participant in the Code since 2020 and we remain engaged in the Code's Taskforce, working groups, and subgroups. We continue to co-chair the Elections working group and have co-chaired the Transparency working group since September 2023.

This sixth report provides detailed insights into the measures we implement to combat disinformation, supported by comprehensive data. Of note during this reporting period:

- We increased the number of fake accounts that we removed by 98% compared to the previous reporting cycle;
- Videos labeled with "creator labeled as AI-generated" and videos labeled with AIGC tag of "AI-generated" increased by 36% and 81% respectively, while videos removed for violating our Edited Media and AI-Generated Content policy dropped by 53%;
- The number of fact-checked videos increased by 114% and the number of videos removed as a result of fact checking assessment increased by 80%.

Several measures extend beyond EU member states, such as in candidate countries and nations with significant diaspora communities, positively contributing to limiting disinformation within the EU.

TikTok remains committed to protecting our community from disinformation, strengthening resilience against misinformation, and upholding transparency and accountability throughout electoral and crisis contexts.

A number of elections took place across Europe in H1 2025, and with that, elevated risks of inauthentic behaviour and attempts to mislead people or our systems in order to influence public discussion. This report details our efforts to safeguard users and protect platform integrity, including:

- Enforcing robust misinformation policies;
- Elevating reliable information from authoritative sources;

- Collaborating with our 12 IFCN-accredited fact-checking partners and other external experts to strengthen our approach.

During this period, we devoted multiple resources to election integrity, including:

- Operating Mission Control Centres for dedicated monitoring;
- Participating in the Code's Rapid Response System to streamline coordination with civil society, fact-checkers, and platforms;
- Launching dedicated Election Centres with localised media literacy campaigns;
- Establishing a new Global Elections Integrity Hub within our Transparency Center, which includes detailed coverage of elections across Europe.

We published four specific post-election chapters in this report documenting our approach to the German Federal Election, Polish Presidential Election, Portuguese Legislative Election, and Romanian Presidential Election. We continue to provide dedicated crisis reports on the ongoing conflicts in Israel/Gaza and Russia/Ukraine, outlining our responses and safeguards.

Our policies

Our Integrity and Authenticity policies are designed to help promote a trustworthy, authentic experience for our users. Our policies cover specific types of misinformation and deceptive behaviours, as well as misleading AI-generated content, conspiracy theories, Covert Influence Operations (CIO) networks, and public safety events like natural disasters. We do not allow false or misleading content that may cause significant harm to individuals or society, regardless of intent. We do not allow misinformation or content about civic and electoral processes that may result in voter interference, disrupt the peaceful transfer of power, or lead to off-platform violence. Our policies are thoughtfully crafted to cover a broad range of content and the constantly changing nature of misinformation trends, often based on what's happening in the world. We also tackle deceptive behaviour by removing accounts that seek to mislead people or engage in platform manipulation.

Enforcing our policies

Disinformation presents unique challenges. It is highly complex, evolves quickly, and often requires context. Our specialised misinformation moderation team receives training to assess, confirm, and take action on harmful misinformation. They also have access to our [independent fact-checking partners](#) and our global database of previously fact-checked claims to help evaluate content accuracy. We place considerable emphasis on proactive detection and automated moderation technology to action violative content. In H1 2025, 86% of the violative videos we removed globally were taken down through automated technology. We use machine learning models to help detect potential misinformation and we rely on automated moderation when our systems have a high degree of confidence that content is violative. To further support proactive moderation at scale, we began testing large language models (LLMs). Because LLMs can comprehend human language and perform highly specific, complex tasks, we are better able to moderate nuanced areas like misinformation by extracting specific misinformation "claims" from videos for our moderators to assess directly or route to our fact-checking partners.

We are transparent with our community about [how we moderate](#) content and what [moderation actions we take](#). This includes details about what content we make [ineligible for the For You Feed](#). We disclose the underlying metrics in this report.

We also address disinformation by removing accounts that repeatedly post misinformation that violates our policies, and have expert teams who continuously monitor potential disinformation campaigns, inauthentic behavior, and influence operations.



Transparency and Scrutiny of Advertising

Under our misinformation advertising policy, we are committed to maintaining a safe and trustworthy environment by taking action against misinformation, such as false, misleading, or unsubstantiated content, and manipulated content which misleads viewers and could harm individuals or society regardless of intent. During H1 2025, we continued to improve and enforce our [granular misinformation ad policies](#) in the EEA.

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. Our [Creator Code of Conduct](#) outlines the standards we expect creators involved in TikTok programs, features, events and campaigns to uphold, both on and off-platform, including in relation to misinformation-related activities.

We continue to engage with external stakeholders in order to increase the effectiveness of our scrutiny of ad placements on TikTok. We have expanded the functionality (including choice and ability) of the TikTok Inventory Filter, our in-house pre-campaign safety tool (which is available in 29 jurisdictions in the EEA), continued to offer third-party brand safety and suitability solutions to our advertisers (such as DoubleVerify, Integral Ad Science and Zefr).

Prohibiting Political Ads

TikTok is first and foremost an entertainment platform, and we're proud to be a place that brings people together through creative and entertaining content. While sharing political beliefs and engaging in political conversation is allowed as organic content on TikTok, our policies prohibit our community, including politicians and political party accounts, from placing [political ads](#) or posting politically [branded content](#). We also prevent [governments, politicians and political party accounts](#) from accessing our monetisation features and campaign fundraising (with a limited exception for government-run public service announcements such as health campaigns).

We have been focusing on enforcement of our political advertising prohibition in advance of the majority of the provisions in the EU Regulation on Transparency and Targeting of Political Advertising applying from October 2025.

By prohibiting political advertising, 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](#) strictly prohibit deceptive behaviors, and we are committed to combating manipulative practices. We remain highly vigilant about the evolving disinformation tactics, techniques, and procedures employed by malicious actors, as outlined in detail in Commitment 14. To effectively combat these threats, we continuously assess and refine our policies, ensuring they remain robust and responsive to emerging challenges in the information ecosystem. Through proactive monitoring and enforcement, we aim to safeguard the integrity of our platform and protect users from harmful influence operations.

We also 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. To counter emerging threats and stay ahead



of evolving challenges, we have expert teams who focus entirely on detecting, investigating, and disrupting covert influence operations. These teams pursue and analyse on-platform signals of deceptive behaviour, as well as leads from external sources. They also collaborate with external intelligence vendors to support specific investigations on a case-by-case basis. In order to provide more regular and detailed updates about the CIOs we disrupt, we have a dedicated transparency report on CIOs, which is [available in TikTok's Transparency Centre](#), and in which we publish information about operations that we have previously removed and that have attempted to return to our platform with new accounts.

We've continued to strengthen our transparency work in Artificial Intelligence (AI) through the Edited Media and AI-Generated Content (AIGC) policy, which addresses the use of content created or modified by AI on our platform. To support authentic and transparent experiences for our community, we require creators to label content that has been either completely generated or significantly edited by AI and disclose when their content shows realistic scenes. We detect AI-generated content through a combination of proactive technologies, alerts from experts and fact-checking partners, searches for clips or keywords related to known AI-generated content, and user reports. Since joining the [Coalition for Content Provenance and Authenticity \(C2PA\)](#) and the [Content Authenticity Initiative \(CAI\)](#) in May 2024, we've continued to collaborate on driving industry adoption of Content Credentials, a technology that helps platforms more easily label AI-generated content.

TikTok is also proud to actively participate in the Code's Rapid Response System, which streamlines the exchange of information among civil society organisations, fact-checkers, and online platforms.

Empowering Users

In addition to taking action on content generated by users that violates our policies, we continuously work to deter misinformation proactively by empowering our community with resources that help them recognise misinformation, critically assess content, and file reports about potentially violative content. We offer our community in Europe easy-to-use in-app and online reporting tools so they can alert us to content or accounts they believe may violate our Community Guidelines or break the law. Content that is reported for being illegal will be reviewed against our policies, and where a violation is detected, the content may be removed globally.

We continue to dedicate resources to expanding our in-app measures that show users additional context on certain content (e.g., natural disasters and rapidly unfolding events), and to redirect them to authoritative information. We make these tools available in 23 EU official languages, and Norwegian and Icelandic for EEA users. For example, during this reporting period, we launched temporary in-app search guides to help users navigate sensitive events with authoritative information, including Pope Francis's health (Italy, Portugal), the Ballymena Riots (Ireland, UK), and natural disasters such as Cyclone Garance (Réunion) and Cyclone Mayotte. These guides connected users to TikTok's Safety Center and authoritative third-party resources on aid and relief support.

We rolled out three new ongoing media literacy and critical thinking campaigns in Germany, Romania, and Poland, in collaboration with fact-checking and media literacy partners. This brings the total number of such campaigns in Europe to 14 countries.

We ran nine temporary media literacy election integrity campaigns, all with in-app Election Centers, in advance of regional elections. Search interventions were seen by users more than 115 million times during the reporting period. And, to better inform us about our approach to upcoming elections, we hosted seven Election Speaker Series, three in EU member states and four in Albania, Belarus, Greenland, and Kosovo, inviting external experts, including from the fact-checking community, to share their insights and market expertise with our internal teams.

We continue to offer greater transparency to users about our systems and integrity and authenticity efforts. Our Transparency Center provides a wealth of information about how we [counter deceptive behaviour](#), protect the integrity of specific [global elections](#), disrupt [Covert Influence Operations](#), and regular updates about broader trust and safety work through the [Transparency Center blog](#).



Empowering the Research Community

We recognise the important role of researchers in helping to identify disinformation trends and practices. We publish quarterly [Community Guidelines Enforcement Reports](#) to provide ongoing insights into the action we take against content and accounts that violate our Community Guidelines, Terms of Service, and Advertising Policies. 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. We maintain, and continue to iterate, our [Research API](#) (providing researchers in Europe with access to public data on content and accounts from our platform) as well as our [Commercial Content API](#) (bringing transparency to paid advertising and other content that is commercial in nature on TikTok) and a Commercial Content Library (a publicly searchable EU ads database with information about paid ads and ad metadata). We also continue to refine the [Virtual Compute Environment](#) (VCE), which offers broader access to user data to qualifying not-for-profit researchers to query and analyse applicable data while ensuring robust security and privacy protections.

We are committed to transparency about how we operate, moderate and recommend content, empower users, and secure our platform. That's why we opened our global Transparency and Accountability Centers (TACs) to invite guests to see first-hand our work to protect the safety and security of the TikTok platform. The TACs offer an opportunity for researchers and other expert audiences to better understand how teams at TikTok go about the critically important work of securing our community's safety, data, and privacy.

Empowering the Fact-Checking Community

TikTok recognises the important contribution of our fact-checking partners in the fight against disinformation. We work closely with 12 [IFCN-accredited](#) fact-checking organisations across the EU, EEA, and wider Europe, which have technical training, resources, and industry-wide insights to impartially assess online misinformation.

Our fact-checking programme incorporates fact-checker input into our broader content moderation efforts. Fact-checkers do not moderate content directly on TikTok, but assess whether a claim is true, false, or unsubstantiated. They also share proactive insight reports that help us detect harmful misinformation and anticipate misinformation trends. This feedback from fact-checkers is relayed to TikTok's moderation teams so that they can ensure it is factored into their moderation work and take the relevant action based on our Community Guidelines. 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 expanding fact-checking repository ensures that our teams and systems fully utilise the insights provided by our fact-checking partners on TikTok.

Looking forward

TikTok remains fully committed to the Code and we look forward to ongoing and meaningful collaboration with the industry, civil society, and EU authorities as we work together to safeguard the integrity of our platforms. By sharing expertise, strengthening policies, and enhancing enforcement mechanisms, we aim to prevent bad actors from exploiting digital spaces through deceptive behaviour and the spread of harmful disinformation.



II. Scrutiny of Ad Placements Commitments 1 - 3



II. Scrutiny of Ad Placements	
Commitment 1	
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> <p>Guidance to support the identification of policies. Improving identification. Improvement of the enforcement of the policies themselves (not the policy wording).</p>	<ul style="list-style-type: none"> Continued to improve and enforce our five granular harmful misinformation ad policies in the EEA. As mentioned in our H2 2024 report, the policies cover: <ul style="list-style-type: none"> Medical Misinformation Dangerous Misinformation Synthetic and Manipulated Media Dangerous Conspiracy Theories Climate Disinformation We continue to engage in the Task-force and its working groups and subgroups such as the working subgroup on Elections (Crisis Response).
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 1.1	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 1.1.1	N/A



SLI 1.1.1 – Numbers by actions enforcing policies above (specify if at page and/or domain level)	N/A			
SLI 1.1.2 -	N/A			

Measure 1.2	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .			
QRE 1.2.1	N/A			
SLI 1.2.1	N/A			
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, 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. We expanded our Inventory Filter which is now available in 29 jurisdictions in the EEA and is embedded directly in TikTok Ads Manager, the main system through which advertisers purchase ads. We have expanded the functionality of this Inventory Filter in various EEA countries. More details can be found here. The Inventory Filter is informed by Industry Standards and policies, which include topics that may be susceptible to disinformation. Additionally, this enabled advertisers to: <ul style="list-style-type: none"> ○ Selectively exclude unwanted or misaligned videos that do not align with their brand safety requirements from appearing next to their ads through TikTok's Video Exclusion List solution. ○ Exclude specific profile pages from serving their Profile Feed ads through TikTok's Profile Feed Exclusion List. • TikTok Pre-bid Brand Safety Solution by Integral Ad Science ("IAS"): Advertisers can filter content based on industry-standard frameworks with all levels of risk (available in France and Germany). Some misinformation content may be captured and filtered out by these industry standard 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 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 (now available in 29 countries in the EEA). Zefr aligns with the Industry Standards. • IAS: Advertisers can measure brand safety, viewability, and invalid traffic on the platform with the IAS Signal platform (post campaign is available in 28 countries in the EEA). As with IAS's pre-bid solution covered above, this aligns with the Industry Standards. • DoubleVerify: We are partnering with DoubleVerify to provide advertisers with media quality measurement for ads. DoubleVerify is working actively with us to expand its suite of brand suitability and media quality solutions on the platform. DoubleVerify is available in 27 EU countries.
<p>Measure 1.4</p>	<p>TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document.</p>



QRE 1.4.1	N/A
Measure 1.5	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 1.5.1	N/A
QRE 1.5.2	N/A
Measure 1.6	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 1.6.1	N/A
QRE 1.6.2	N/A
QRE 1.6.3	N/A
QRE 1.6.4	N/A
SLI 1.6.1	N/A



II. Scrutiny of Ad Placements	
Commitment 2	
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 enforce and improve our five granular harmful misinformation ad policies in the EEA. As mentioned in our H2 2024 report, the policies cover: <ul style="list-style-type: none"> Medical Misinformation Dangerous Misinformation Synthetic and Manipulated Media Dangerous Conspiracy Theories Climate Misinformation Enabled advertisers to selectively exclude unwanted or misaligned videos that do not align with their brand safety requirements from appearing next to their ads through TikTok's Video Exclusion List solution. Enabled advertisers to exclude specific profile pages from serving their Profile Feed ads through TikTok's Profile Feed Exclusion List. We continue to engage in the Task-force and its working groups and subgroups such as the working subgroup on Elections (Crisis Response).
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A



Measure 2.1		
QRE 2.1.1	Paid ads are subject to our strict ad policies , which specifically prohibit misleading, inauthentic, and deceptive behaviours. Ads are reviewed against these policies before being allowed on our platform. In order to improve our existing ad policies, we launched four more granular policies in the EEA in 2023 (covering Medical Misinformation, Dangerous Misinformation, Synthetic and Manipulated Media, and Dangerous Conspiracy Theories), which advertisers also need to comply with. In December 2024, we launched a fifth granular policy covering Climate Misinformation.	
SLI 2.1.1 – Numbers by actions enforcing policies above	<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 political content policies, as well as our five granular policies on Medical Misinformation, Dangerous Misinformation, Synthetic and Manipulated Media, Dangerous Conspiracy Theories, and Climate Misinformation. We launched our Climate Misinformation policy in December 2024.</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 for these additional misinformation policies, the removal is counted under the older policy. Therefore, the second column below shows only the number of ads removed where the sole reason was one of these five 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) 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 political content ad policy	Number of ad removals under the five granular misinformation ad policies
Member States		
Austria	1,634	11



Belgium	2,447	4
Bulgaria	880	9
Croatia	705	0
Cyprus	585	0
Czech Republic	859	0
Denmark	796	2
Estonia	307	0
Finland	1,033	2
France	16,026	46
Germany	18,041	72
Greece	2,420	20
Hungary	1,647	111
Ireland	1,263	8
Italy	8,150	27
Latvia	795	2
Lithuania	521	4
Luxembourg	250	1
Malta	0	0
Netherlands	3,028	30



Poland	5,699	19
Portugal	1,430	1
Romania	13,989	23
Slovakia	500	2
Slovenia	230	2
Spain	6,526	54
Sweden	1,659	8
Iceland	3	0
Liechtenstein	0	0
Norway	1,071	3
Total EU	91,420	458
Total EEA	92,494	461

Measure 2.2	
QRE 2.2.1	<p>In order to identify content and sources that breach our ad policies, ads go through moderation prior to going “live” on the platform.</p> <p>TikTok places considerable emphasis on proactive moderation of advertisements. Advertisements and advertiser accounts are reviewed against our Advertising Policies at the pre-posting and post-posting stage through a combination of automated and human moderation.</p>



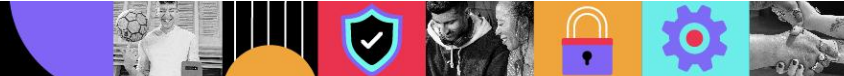
	<p>The majority of ads that violate our misinformation policies would have been removed under our existing policies. Our granular advertising policies currently cover:</p> <ul style="list-style-type: none"> • Dangerous Misinformation • Dangerous Conspiracy Theories • Medical Misinformation • Synthetic and Manipulated Media • Climate Misinformation <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 undergo 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, ads go through moderation prior to going “live” on the platform.</p> <p>TikTok places considerable emphasis on proactive moderation of advertisements. Advertisements and advertiser accounts are reviewed against our Advertising Policies at the pre-posting and post-posting stage through a combination of automated and human moderation.</p> <p>The majority of ads that violate our misinformation policies would have been removed under our existing policies. Our granular advertising policies currently cover:</p> <ul style="list-style-type: none"> • Dangerous Misinformation • Dangerous Conspiracy Theories • Medical Misinformation • Synthetic and Manipulated Media • Climate Misinformation



	<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 political content policies, as well as our more granular misinformation ad policies, including the impressions of those ads in this report. We launched our Climate Misinformation policy in December 2024 and therefore have been able to include data in this report for the full reporting period of H1 2025.</p>			
	Number of ad removals under the political content ad policy	Number of ad removals under the five granular misinformation ad policies	Number of impressions for ads removed under the political content ad policy	Number of impressions for ads removed under the five granular misinformation ad policies
Member States				
Austria	1,634	11	2,778,373	12,798
Belgium	2,447	4	9,857,484	9,532
Bulgaria	880	9	134,516	0
Croatia	705	0	50,245	0
Cyprus	585	0	759,396	0
Czech Republic	859	0	574,781	0
Denmark	796	2	1,733,369	591
Estonia	307	0	123,793	0



Finland	1,033	2	2,689,290	406
France	16,026	46	20,117,190	2,613
Germany	18,041	72	13,135,219	198,032
Greece	2,420	20	1,046,084	2,409
Hungary	1,647	111	2,475,500	155,048
Ireland	1,263	8	6,118,934	23,761
Italy	8,150	27	22,568,047	17,614
Latvia	795	2	309,633	49,404
Lithuania	521	4	1,569,605	0
Luxembourg	250	1	19,487	0
Malta	0	0	0	0
Netherlands	3,028	30	1,346,613	22,471
Poland	5,699	19	2,811,216	43,493
Portugal	1,430	1	1,034,542	0
Romania	13,989	23	13,399,159	90,558
Slovakia	500	2	49,874	0
Slovenia	230	2	29,448	0
Spain	6,526	54	23,225,371	7,266
Sweden	1,659	8	4,710,643	4,158



Iceland	3	0	0	0
Liechtenstein	0	0	0	0
Norway	1,071	3	4,279,908	0
Total EU	89,789	458	132,667,812	640,154
Total EEA	90,860	461	136,947,720	640,154

Measure 2.4	
QRE 2.4.1	<p>We are clear with advertisers that their ads must comply with our strict ad policies (see TikTok Business Help Centre). We explain that all ads are reviewed before being uploaded on our platform - usually within 24 hours. 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> <p>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 and/or sent by email (if they have provided a valid email address), 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.</p> <p>As part of our overarching DSA compliance programme, we improved how we notify and increase transparency to our advertisers. Notifications of restrictions include the restriction itself, reason for restriction, whether we made that decision by automated means, how we came to detect the violation (e.g. as a result of a user report or proactive TikTok initiatives) and what their rights of redress are. Advertisers can access online functionality to appeal restrictions on their account or ads. These appeals are then also reviewed against our ad policies and additional information could be provided to advertisers to help them understand the violation and what to do about it.</p>
SLI 2.4.1	<p>We are pleased to be able to share the number of appeals for ads removed under our political content ad policies and our five granular misinformation ad policies as well as the number of respective overturns.</p>



	Number of appeals for ads removed under the the five granular misinformation ad policies	Number of appeals for ads removed under the political content policy	Number of overturns following appeals under the five more granular misinformation policies	Number of overturns following appeals under the political content policy
Member States				
Austria	0	87	0	59
Belgium	0	84	0	48
Bulgaria	0	8	0	4
Croatia	0	0	0	2
Cyprus	0	6	0	3
Czech Republic	0	215	0	8
Denmark	0	109	0	57
Estonia	0	6	0	1
Finland	0	108	0	49
France	0	154	0	99
Germany	0	105	0	59
Greece	0	36	0	17
Hungary	0	65	0	36
Ireland	0	207	0	0
Italy	0	302	0	246
Latvia	0	10	0	6



Lithuania	0	10	0	6
Luxembourg	0	0	0	0
Malta	0	0	0	0
Netherlands	0	132	0	58
Poland	1	153	0	113
Portugal	0	105	0	79
Romania	0	41	0	23
Slovakia	0	10	0	3
Slovenia	0	8	0	2
Spain	0	160	0	80
Sweden	0	96	0	38
Iceland	0	0	0	0
Liechtenstein	0	0	0	0
Norway	0	91	0	44
Total EU	1	2,217	0	1,096
Total EEA	1	2,308	0	1,140



II. Scrutiny of Ad Placements	
Commitment 3	
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].	We continue to engage in the Task force and all its working groups and subgroups such as the working subgroup on Elections (Crisis Response).
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A



Measure 3.1	
QRE 3.1.1	<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>We also continue to be actively involved in the Task-force working group for Chapter 2, specifically the working subgroup on Elections (Crisis Response) which we co-chaired. We work 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>
Measure 3.2	
QRE 3.2.1	<p>We work with industry partners to discuss common standards and definitions to support consistency of categorising content, adjacency and measurement relevant topics, in appropriate fora. 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 subgroups set up for insights sharing between signatories and the Commission.</p>
Measure 3.3	
QRE 3.3.1	<p>We continue to work closely with IAB Sweden, IAB Ireland, and other organisations such as TAG in the EEA and globally.</p>



III. Political Advertising Commitments 4 - 13



III. Political Advertising	
Commitment 4	
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]	TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document .
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 4.1	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
Measure 4.2	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 4.1.1 (for measures 4.1 and 4.2)	N/A
QRE 4.1.2 (for measures 4.1 and 4.2)	N/A



III. Political Advertising	
Commitment 5	
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]	TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document .
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 5.1	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 5.1.1	N/A



III. Political Advertising	
Commitment 6	
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]	TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document .
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 6.1	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 6.1.1	N/A
Measure 6.2	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 6.2.1	N/A
QRE 6.2.2	N/A



SLI 6.2.1 – numbers for actions enforcing policies above	N/A		
Member States	N/A	N/A	N/A
Total EU	N/A	N/A	N/A
Total EEA	N/A	N/A	N/A

Measure 6.3	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 6.3.1	N/A
Measure 6.4	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 6.4.1	N/A
Measure 6.5	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 6.5.1	N/A



III. Political Advertising	
Commitment 7	
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]	TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document .
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 7.1	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 7.1.1	N/A
SLI 7.1.1 – numbers for actions enforcing policies above (comparable metrics as for SLI 6.2.1)	N/A



Measure 7.2	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 7.2.1	N/A
QRE 7.2.2	N/A
Measure 7.3	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 7.3.1	N/A
QRE 7.3.2	N/A
Measure 7.4	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 7.4.1	N/A



III. Political Advertising	
Commitment 8	
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]	TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document .
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 8.1	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
Measure 8.2	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 8.2.1 (for measures 8.1 and 8.2)	N/A



III. Political Advertising	
Commitment 9	
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]	TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document .
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 9.1	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
Measure 9.2	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 9.2.1 (for measures 9.1 and 9.2)	N/A



III. Political Advertising	
Commitment 10	
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]	TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document .
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 10.1	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
Measure 10.2	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 10.2.1 (for measures 10.1 and 10.2)	N/A



III. Political Advertising	
Commitment 11	
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]	TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document .
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 11.1	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
Measure 11.2	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
Measure 11.3	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
Measure 11.4	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .



QRE 11.1.1 (for measures 11.1-11.4)	N/A
QRE 11.4.1	N/A

III. Political Advertising	
Commitment 12	
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]	TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document .
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 12.1	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
Measure 12.2	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .



Measure 12.3	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 12.1.1 (for measures 12.1-12.3)	N/A

III. Political Advertising	
Commitment 13	
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]	TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document .
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 13.1	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
Measure 13.2	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .

Measure 13.3	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 13.1.1 (for measures 13.1-13.3)	N/A



IV. Integrity of Services

Commitments 14 - 16



IV. Integrity of Services

Commitment 14

In order to limit impermissible manipulative behaviours and practices across their services, Relevant Signatories commit to put in place or further bolster policies to address both misinformation and disinformation across their services, and to agree on a cross-service understanding of manipulative behaviours, actors and practices not permitted on their services. Such behaviours and practices, which should periodically be reviewed in light with the latest evidence on the conducts and TTPs employed by malicious actors, such as the AMITT Disinformation Tactics, Techniques and Procedures Framework, include:

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

- 1. Creation of inauthentic accounts or botnets (which may include automated, partially automated, or non-automated accounts)
- 2. Use of fake / inauthentic reactions (e.g. likes, up votes, comments)
- 3. Use of fake followers or subscribers
- 4. Creation of inauthentic pages, groups, chat groups, fora, or domains
- 5. Account hijacking or impersonation

The following TTPs pertain to the dissemination of content created in the context of a disinformation campaign, which may or may not include some forms of targeting or attempting to silence opposing views. Relevant TTPs include:

- 6. Deliberately targeting vulnerable recipients (e.g. via personalised 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

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"> • Building on our AI-generated content label for creators, and implementation of C2PA Content Credentials, we completed our AIGC media literacy campaign series in Mexico and the UK. These campaigns in Brazil, Germany, France, Mexico and the UK, which ran across H2 2024 and H1 2025, were developed with guidance from expert organisations like Mediawise and WITNESS to teach our community how to spot and label AI generated content. They reached more than 90M users globally, including more than 27M in Mexico and 10M in the UK. • Continued to join industry partners as a party to the “Tech Accord to Combat Deceptive Use of AI in 2024 Elections” which is a joint commitment to combat the deceptive use of AI in elections. • Continued to participate in the working groups on the integrity of services and Generative AI. • We have continued to enhance our ability to detect covert influence operations. To provide more regular and detailed updates about the covert influence operations we disrupt, we have a dedicated Transparency Report on covert influence operations, which is available in TikTok’s Transparency Centre. In this report, we include information about operations that we have previously removed and that have attempted to return to our platform with new accounts. • We continue to update and refine our policies around Covert Influence Operations in order to stay agile to changing behaviours and tactics on the platform and to ensure more granular detail is enshrined in our policy rationales.
<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>N/A</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<p>N/A</p>
<p>Measure 14.1</p>	



<p>QRE 14.1.1</p>	<p>As well as our Integrity and Authenticity policies in our Community Guidelines, which safeguard against harmful misinformation (see QRE 18.2.1), our Integrity and Authenticity policies also expressly prohibit deceptive behaviours. Our policies on deceptive behaviours relate to the TTPs as follows:</p> <p><i>TTPs which pertain to the creation of assets for the purpose of a disinformation campaign, and the ways to make these assets seem credible:</i></p> <p>Creation of inauthentic accounts or botnets (which may include automated, partially automated, or non-automated accounts)</p> <p>Our Integrity and Authenticity 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.</p> <p>We do not allow spam, including:</p> <ul style="list-style-type: none"> • Operating large networks of accounts controlled by a single entity, or through automation; • Bulk distribution of a high volume of spam; and • Manipulation of engagement signals to amplify the reach of certain content, or buying and selling followers, particularly for financial purposes <p>We also do not allow impersonation, including:</p> <ul style="list-style-type: none"> • Accounts that pose as another real person or entity without disclosing that they are a fan or parody account in the account name, such as using someone's name, biographical details, content, or image without disclosing it • Presenting as a person or entity that does not exist (a fake persona) with a demonstrated intent to mislead others on the platform <p>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.</p>
--------------------------	---

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

Our Integrity and Authenticity policies, which address **fake engagement**, do not allow the trade or marketing of services that attempt to artificially increase engagement or deceive TikTok's recommendation system. We do not allow our users to:

- facilitate the trade or marketing 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 (to increase gifts, followers, likes, views, or other engagement metrics) 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

Again, 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 continue to develop our policies to ensure that impersonation of entities (such as businesses or educational institutions, for example) is prohibited and that accounts which impersonate people or entities who are not on the platform are also prohibited. We also issue warnings to users of suspected impersonation accounts and do not recommend those accounts on our For You Feed.



We also have a number of policies that address account hijacking. Our privacy and security policies under our Community Guidelines expressly prohibit users from providing access to their account credentials to others or enabling others to conduct activities against our Community Guidelines. 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.



	<p>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 reestablish a presence on our platform. That is why we take continuous action against these attempts, including banning accounts found to be linked with previously disrupted networks. 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 have published details of all the CIO networks we identified and removed in H1 2025 in a dedicated monthly report within our Transparency Centre here.</p> <p>In H1 2025, through our Deceptive Behaviours policies we worked on a number of initiatives that sought to continue developing and adapting our strategies at combatting manipulative behaviours and practices. We continue to make progress through several updates and development schemes.</p> <p>Use “hack and leak” operation (which may or may not include doctored content)</p> <p>We have a number of policies that address hack-and-leak related threats (some examples are below):</p> <ul style="list-style-type: none"> • Our hack and leak policy, which aims to further reduce 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. • Our CIO policy addresses use of leaked documents to sway public opinion as part of a wider operation. • Our Edited Media and AI-Generated Content (AIGC) policy captures materials that have been digitally altered without an appropriate disclosure. • Our harmful misinformation policies combat conspiracy theories related to unfolding events and dangerous misinformation.
--	--



- Our Trade of Regulated Goods and Services policy prohibits the trading of hacked goods.

Deceptive manipulated media (e.g. “deep fakes”, “cheap fakes”...)

Our ‘Edited Media and AI-Generated Content (AIGC)’ policy includes commonly used and easily understood language when referring to AIGC, and outlines our existing prohibitions on AIGC showing fake authoritative sources or crisis events, or falsely showing public figures in certain contexts, including being bullied, making an endorsement, or being endorsed. We also do not allow content that contains the likeness of young people, or the likeness of adult private figures used without their permission.

For the purposes of our policy, AIGC refers to content created or modified by artificial intelligence (AI) technology or machine-learning processes, which may include images of real people, and may show highly realistic-appearing scenes, or use a particular artistic style, such as a painting, cartoons, or anime. ‘Significantly edited content’ is content that shows people doing or saying something they did not do or say, or altering their appearance in a way that makes them difficult to recognise or identify. Misleading AIGC or edited media is audio or visual content that has been edited, including by combining different clips together, to change the composition, sequencing, or timing in a way that alters the meaning of the content and could mislead viewers about the truth of real-world events.

In accordance with our policy, we prohibit AIGC, which features:

- The likeness of young people or realistic-appearing people under the age of 18.
- The likeness of adult private figures, if we become aware that it was used without their permission.
- Misleading AIGC or edited media that falsely show:
 - Content made to seem as if it comes from an authoritative source, such as a reputable news organisation.
 - A crisis event, such as a conflict or natural disaster
 - A public figure who is:
 - being degraded or harassed, or engaging in criminal or antisocial behaviour.



	<ul style="list-style-type: none"> ■ taking a position on a political issue, commercial product, or a matter of public importance (such as an election). ■ being politically endorsed or condemned by an individual or group. <p>As AI evolves, we continue to invest in combating harmful AIGC by evolving our proactive detection models, consulting with experts, and partnering with peers on shared solutions.</p> <p>Non-transparent compensated messages or promotions by influencers</p> <p>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 made this requirement even clearer to users in our Commercial Disclosures and Paid Promotion policy in our March 2023 Community Guidelines refresh by increasing the information around our policing of this policy and providing specific examples.</p> <p>We also don't allow paid political advertising. This includes creators being compensated for making branded political content, and the use of other promotional tools on the platform, such as Promote. We prohibit advertising of any kind by political figures and entities, and suspected paid political advertising is ineligible for the For You feed.</p> <p>In addition to branded content policies, our CIO policy can also apply to non-transparent compensated messages or promotions by influencers where it is found that those messages or promotions formed part of a covert influence campaign.</p>
--	--



QRE 14.1.2

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 *before* they are reported to us by users or third parties.

For instance, we take proactive measures to prevent inauthentic or spam accounts from being created. Thus, we have created and used detection models and rule engines that:

- 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).

We also manually monitor user reports of inauthentic accounts in order to detect larger clusters or similar inauthentic behaviours.

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 in assessing and addressing identified violations. We provide our moderation teams with detailed guidance on how to apply the Integrity and Authenticity policies in our Community Guidelines, including providing case banks of harmful misinformation claims to support their moderation work, and allowing them to route new or evolving content to our fact-checking partners for assessment.

In addition, where content reaches certain popularity levels in terms of the number of video views, it will be flagged for further review. Such a 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 Community Guidelines including our Integrity and Authenticity policies.

Furthermore, during the reporting period, we improved automated detection and enforcement of our 'Edited Media and AI-Generated Content (AIGC)' policy, effectively increasing the number of videos removed for policy violations. This also decreased the number of visitors per video over the reporting period, demonstrating an effective control strategy as the scope of enforcement increased.



	<p>We have also set up specifically-trained teams that are focused on investigating and detecting CIO on our Platform. We've built international trust and safety teams with specialized expertise across threat intelligence, security, law enforcement, and data science to work on influence operations full-time. These teams continuously pursue and analyse on-platform signals of deceptive behaviour, as well as leads from external sources. They also collaborate with external intelligence vendors to support specific investigations on a case-by-case basis. 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>Accounts that engage in influence operations often avoid posting content that would be violative of platforms' guidelines by itself. That's why we focus on accounts' behaviour and technical linkages when analysing them, specifically looking for evidence that:</p> <ul style="list-style-type: none"> • They are <u>coordinating with each other</u>. For example, they are operated by the same entity, share technical similarities like using the same devices, or work together to spread the same narrative. • They are <u>misleading our systems or users</u>. For example, they are trying to conceal their actual location or use fake personas to pose as someone they're not. • They are attempting to <u>manipulate or corrupt public debate</u> to impact the decision-making, beliefs, and opinions of a community. For example, they are attempting to shape discourse around an election or conflict. <p>These criteria are aligned with industry standards and guidance from the experts we regularly consult with. They're particularly important to help us distinguish malicious, inauthentic coordination from authentic interactions that are part of healthy and open communities. For example, it would not violate our policies if a group of people authentically worked together to raise awareness or campaign for a social cause, or express a shared opinion (including political views). However, multiple accounts deceptively working together to spread similar messages in an attempt to influence public discussions would be prohibited and disrupted.</p>
--	---



Measure 14.2	
QRE 14.2.1	<p>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).</p> <p>The implementation of these policies is also ensured through enforcement measures applied in all Member States.</p> <p>CIO investigations are resource-intensive and require in-depth analysis to ensure high confidence in proposed actions. Where our teams have the necessary high degree of confidence that an account is engaged in CIO or is connected to networks we took down in the past as part of a CIO, it is removed from our Platform.</p> <p>Similarly, where our teams have a high degree of confidence that specific content violates one of our TTPs-related policies (See QRE 14.1.1), such content is removed from TikTok.</p> <p>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.</p>



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 ratio of monthly average of fake accounts over of monthly active users, based on the latest publication 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		
	Number 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				Ratio of monthly average of Fake accounts over monthly active users		
Member States								
Austria	285,956	2,405,075						
Belgium	307,720	7,310,366						
Bulgaria	44,457	311,881						
Croatia	110,715	832,216						
Cyprus	22,380	137,466						
Czech Republic	74,789	222,272						
Denmark	477,253	661,003						
Estonia	120,618	130,255						
Finland	6,739,153	23,272,143						
France	218,065	163,289						
Germany	3,061,413	23,462,309						



Greece	401,172	829,495						
Hungary	203,010	241,844						
Ireland	511,825	384,711						
Italy	2,125,801	18,134,280						
Latvia	16,648	157,713						
Lithuania	139,076	169,438						
Luxembourg	85,647	127,440						
Malta	47,124	134,032						
Netherlands	907,262	460,094						
Poland	679,441	5,577,067						
Portugal	359,384	283,725						
Romania	242,048	2,628,711						
Slovakia	393,046	2,669,356						
Slovenia	134,065	94,225						
Spain	1,001,039	5,555,675						
Sweden	515,924	2,157,008						
Iceland	14,715	6,444						
Liechtenstein	11,867	9,343						
Norway	345,798	77,624						



Total EU	19,225,031	98,513,089				1.896%		
Total EEA	19,597,411	98,606,500						

TTP OR ACTION 2	TTP no. 2: Use of fake / inauthentic reactions (e.g. likes, up votes, comments)							
	Methodology of data measurement: 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.							
	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4				
	Number 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	13,131,306	15,555,848						
Belgium	17,889,142	24,913,181						



Bulgaria	6,083,357	24,981,658		
Croatia	1,936,664	8,908,266		
Cyprus	6,728,038	4,551,392		
Czech Republic	4,621,360	18,639,686		
Denmark	4,599,038	8,859,796		
Estonia	1,223,666	4,214,784		
Finland	123,447,223	164,578,253		
France	4,452,036	9,042,193		
Germany	104,372,738	173,915,566		
Greece	17,780,664	31,043,396		
Hungary	3,569,106	13,886,460		



Ireland	5,275,248	12,978,143		
Italy	76,731,830	444,513,176		
Latvia	1,456,849	5,925,459		
Lithuania	1,537,828	7,615,832		
Luxembourg	1,657,907	3,697,321		
Malta	1,443,459	2,274,413		
Netherlands	33,206,716	169,029,147		
Poland	14,551,480	68,507,115		
Portugal	10,223,131	26,580,434		
Romania	23,781,565	74,755,615		
Slovakia	1,564,271	14,313,702		



Slovenia	619,870	3,483,149		
Spain	42,920,611	96,571,232		
Sweden	17,562,119	19,099,488		
Iceland	355,516	889,888		
Liechtenstein	21,916	63,168		
Norway	8,735,563	8,205,011		
Total EU	542,367,222	1,452,434,705		
Total EEA	551,480,217	1,461,592,772		

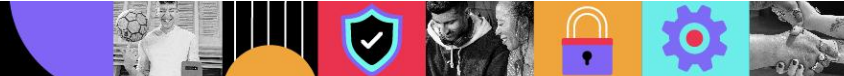
TTP OR ACTION 3	<p>TTP No. 3: Use of fake followers or subscribers</p> <p>Methodology of data measurement:</p> <p>We based the number of fake followers that we removed on the country of registration of the user. We also based the number of fake followers prevented on the country of registration of the user.</p>
------------------------	--



	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4
	Number 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	670,291	11,391,317		
Belgium	1,074,979	10,697,049		
Bulgaria	144,607	11,221,195		
Croatia	151,082	5,108,277		
Cyprus	90,518	3,221,280		



Czech Republic	434,495	8,334,193		
Denmark	229,824	6,161,877		
Estonia	41,314	3,291,374		
Finland	14,804,359	309,132,404		
France	203,317	6,112,202		
Germany	11,530,622	128,451,770		
Greece	305,669	13,299,869		
Hungary	203,669	8,715,303		
Ireland	249,543	14,912,513		
Italy	5,725,474	72,644,339		
Latvia	67,811	3,652,638		



Lithuania	167,115	4,952,989		
Luxembourg	49,821	3,054,641		
Malta	23,534	2,195,248		
Netherlands	1,546,478	17,159,873		
Poland	874,585	26,061,316		
Portugal	501,505	11,311,310		
Romania	1,839,900	27,531,979		
Slovakia	125,472	8,268,587		
Slovenia	36,946	920,490		
Spain	3,460,169	51,652,944		
Sweden	606,091	14,185,279		



Iceland	16,011	1,016,831		
Liechtenstein	12,791	85,185		
Norway	258,701	4,396,839		
Total EU	45,159,190	783,642,256		
Total EEA	45,446,693	789,141,111		

TTP OR ACTION 4	TTP No. 4: 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.			
------------------------	---	--	--	--

TTP OR ACTION 5	TTP No. 5: Account hijacking or impersonation Methodology of data measurement: 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 ratio of monthly average impersonation accounts banned over monthly active users, based on the latest publication of monthly active users, in order to better reflect TTPs related content in relation to overall content on the service.			
	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4



	Number 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 over monthly active users
List actions per member states (see example table above)				
Austria	416			
Belgium	764			
Bulgaria	368			
Croatia	171			
Cyprus	153			
Czech Republic	378			
Denmark	294			
Estonia	63			
Finland	210			
France	5,303			
Germany	5,889			



Greece	473			
Hungary	336			
Ireland	399			
Italy	1,875			
Latvia	117			
Lithuania	205			
Luxembourg	79			
Malta	0			
Netherlands	2,612			
Poland	1,839			
Portugal	623			
Romania	1,180			
Slovakia	172			
Slovenia	128			
Spain	1,560			
Sweden	656			
Iceland	28			
Liechtenstein	0			



Norway	297			
Total EU	26,263			0.0026%
Total EEA	26,588			

TTP OR ACTION 6	TTP No. 6. Deliberately targeting vulnerable recipients (e.g. via personalised advertising, location spoofing or obfuscation) Methodology of data measurement: <p>The number of new CIO network discoveries found to be targeting EU markets relates to our public disclosures for the period January 1st 2025 to June 30th 2025. We have categorised disrupted CIO networks by the country we assess that the network targeted. We have included any network which we assess to have targeted one or more European markets, or have operated from an EU market. We publish all of the CIO networks we identify and remove within our transparency reports here.</p> <p>CIO networks identified and removed are detailed below, including the assessed geographic location of network operation and the assessed target audience of the network, which we assess via 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
Assessed Network Operating Location	Number of instances of identified TTPs and actions taken by type	Interaction/ engagement before action	Views/ impressions after action	Interaction/ engagement after action	Trends on targeted audiences
January-June 2025					



China	2,029 removed accounts	Accounts within the network had 2,844,039 cumulative followers as at the date of removal	Not Measured	Not Measured	We assess that this network operated from China and targeted a Chinese-speaking audience globally. The individuals behind this network created inauthentic accounts in order to promote Chinese economic, political and technological superiority. The network created personas advertising financial advice in order to build an audience. The network used technical means to obfuscate its location.	
Ukraine	28,713 removed accounts	Accounts within the network had 300,456 cumulative followers as at the date of removal	Not measured	Not measured	We assess that this network operated from Ukraine and targeted audiences in Russia, Georgia, Croatia, and Belarus. The individuals behind this network created inauthentic accounts to undermine political candidates favoring Russian-aligned agendas, amplify anti-government protests, and incite ethnic hatred. We assess that the network used off-platform generative artificial intelligence tools in order to create fictitious user avatars.	



Germany	40 removed accounts	Accounts within the network had 213,345 cumulative followers as at the date of removal	Not measured	Not measured	We assess that this network operated from Germany and targeted a German audience. The individuals behind this network created inauthentic accounts in order to amplify content supporting the political party "Alternative for Germany (AfD)." A large proportion of the network's accounts were found to use the word "news" or "nachricht" in their handle or nickname.	
Germany	17 removed accounts	Accounts within the network had 6,412 cumulative followers as at the date of removal	Not measured	Not measured	We assess that this network operated from Germany and targeted a German audience. The individuals behind this network created inauthentic accounts in order to promote the "Bündnis Sahra Wagenknecht (BSW)" Party within the context of the 2025 German Federal elections. The network was found to alternate between posting apolitical and political content in order to drive engagement.	



Germany	14 removed accounts	Accounts within the network had 164,573 cumulative followers as at the date of removal.	Not measured	Not measured	We assess that this network operated from Germany and targeted a German audience. The individuals behind this network created inauthentic accounts in order to promote the political party "Alternative for Germany (AfD)". The accounts used Smurf avatars and were observed to rebrand their accounts and alternate content in order to gain engagement.	
Poland	12 removed accounts	Accounts within the network had 10,252 cumulative followers as at the date of removal.	Not measured	Not measured	We assess that this network operated from Poland and targeted a Polish audience. The individuals behind this network created inauthentic accounts in order to make coordinated and directed posts supporting a Polish politician. The network was found to strategically synchronise activity/content across multiple platforms through hashtags and the timing of posts.	



Germany	9 removed accounts	Accounts within the network had 11,964 cumulative followers as at the date of removal	Not measured	Not measured	We assess that this network operated from Germany and targeted audiences in Germany and Belgium in order to spread conspiracy theories suggesting that the German Federal Republic is illegitimate. The network was found to redirect users to off-platform links which asked users to provide their personal data.	
Togo	129 removed accounts	Accounts within the network had 6,581,841 cumulative followers as at the date of removal	Not measured	Not measured	We assess that this network operated from Togo and targeted a French-speaking audience in West Africa and France. The individuals behind this network created inauthentic accounts in order to undermine France's foreign policies in West Africa. The network presented its accounts and content in a news-like format in an attempt to increase its credibility.	



Romania	60 removed accounts	Accounts within the network had 23,822 cumulative followers as at the date of removal	Not measured	Not measured	We assess that this network operated from Romania and targeted a Romanian audience. The individuals behind this network created inauthentic accounts in order to amplify certain narratives, attempting to manipulate Romanian elections discourse. The network was found to create fictitious personas in order to post comments and content aligned with its strategic goal.	
Poland	49 removed accounts	Accounts within the network had 11,424 cumulative followers as at the date of removal.	Not measured	Not measured	We assess that this network operated from Poland and targeted a Polish audience. The individuals behind this network created inauthentic accounts in order to discredit the current government within the context of the 2025 Polish presidential election. The network was found to post videos that exploited the Volhynia Massacre and other sensitive historical topics to promote Eurosceptic, anti-Ukrainian, and anti-Semitic narratives.	



Romania	27 removed accounts	Accounts within the network had 9,474 cumulative followers as at the date of removal	Not measured	Not measured	We assess that this network operated from Romania and targeted a Romanian audience. The individuals behind this network created inauthentic accounts in order to amplify certain narratives, attempting to manipulate Romanian elections discourse. The network was found to create accounts with generic handles and avatars which it presented as news accounts.	
Ukraine	20 removed accounts	Accounts within the network had 200,048 cumulative followers as at the date of removal.	Not measured	Not measured	We assess that this network operated from Ukraine and targeted audiences in Germany and Ukraine. The individuals behind this network created inauthentic accounts in order to promote anti-Russian viewpoints, within the context of the war between Russia and Ukraine. The network started by targeting a domestic Ukrainian audience but then changed the language used in its videos in order to target a German audience.	



Poland	16 removed accounts	Accounts within the network had 14,743 cumulative followers as at the date of removal.	Not measured	Not measured	We assess that this network operated from Poland and targeted a Polish audience. The individuals behind this network created inauthentic accounts in order to promote nationalistic viewpoints that criticized Poland's engagement with the EU and aid to Ukraine, within the context of the 2025 Polish presidential election. The network systematically recycled content throughout its accounts in order to further spread its messaging.	
Iran	10 removed accounts	Accounts within the network had 4,547 cumulative followers as at the date of removal.	Not measured	Not measured	We assess that this network operated from Iran and targeted US and European audiences. The individuals behind this network created inauthentic personas and news accounts in order to deliver curated content aligned with Iranian foreign policy objectives. Accounts within the network attempted to impersonate official accounts belonging to the Trump administration.	



Unidentified	9 removed accounts	Accounts within the network had 4,164 cumulative followers as at the date of removal.	Not measured	Not measured	We assess that this network targeted a Portuguese audience. The individuals behind this network created inauthentic accounts in order to promote the Socialist Party and undermine the Social Democratic Party, within the context of the 2025 Portuguese election. This network masked its operating location through advanced operational security.	
Russia	116 removed accounts	Accounts within the network had 4,372 cumulative followers as at the date of removal.	Not measured	Not measured	We assess that this network operated from Russia and targeted a European audience. The individuals behind this network created inauthentic accounts posing as journalists from established European news agencies in order to amplify narratives undermining Moldova's government and Moldova's European Union candidate status. The network was found to be using location obfuscation services in order to hide its true operating location.	



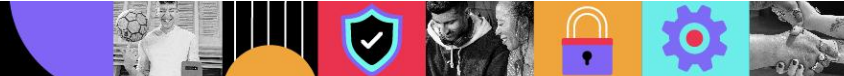
TTP OR ACTION 7	TTP No. 7: Deploy deceptive manipulated media (e.g. “deep fakes”, “cheap fakes”...) We have based the following numbers on the country in which the video was posted: videos removed because of violations of the Edited Media and AI-Generated Content (AIGC) policy. The number of views of videos removed because of violation of each of these policies is based on the approximate location of the user.			
Member States	Number of videos removed because of violation of Edited Media and AI-Generated Content (AIGC) policy	Number of views of videos removed because of Edited Media and AI-Generated Content (AIGC) policy	Number of unique videos labelled with AIGC tag of "Creator labeled as AI-generated"	Number of unique videos labelled with AIGC tag of "AI-generated"
Austria	585	1,786,611	152,577	64,205
Belgium	691	13,473,808	190,690	119,828
Bulgaria	261	16,896	154,476	170,804
Croatia	109	348,415	36,223	26,505
Cyprus	155	1,125,052	84,032	21,199
Czech Republic	356	3,259,466	99,825	149,017
Denmark	331	104,872	61,313	42,289



Estonia	89	262,860	14,320	13,143
Finland	142	1,719,209	85,906	65,726
France	4,373	47,569,470	1,909,743	721,564
Germany	5,389	50,209,813	2,095,417	827,880
Greece	648	2,412,820	232,227	57,603
Hungary	95	32,201	87,799	154,799
Ireland	250	80,522	41,863	43,655
Italy	2,510	6,572,802	918,363	688,389
Latvia	228	403,046	43,707	29,617
Lithuania	168	6,834,539	41,177	32,859



Luxembourg	37	102,103	30,049	6,514
Malta	31	1,462	14,465	7,018
Netherlands	988	2,127,647	324,171	115,936
Poland	655	6,968,424	288,662	501,209
Portugal	662	822,977	195,221	159,689
Romania	2,520	10,019,149	382,348	302,970
Slovakia	113	542,335	29,759	83,055
Slovenia	258	45,635	16,300	10,494
Spain	2,020	55,973,123	966,947	870,721
Sweden	549	402,955	196,366	127,889



Iceland	14	226	4,243	4,957
Liechtenstein	0	0	144	67
Norway	272	739,044	67,870	50,753
Total EU	24,213	213,218,212	8,693,946	5,414,577
Total EEA	24,499	213,957,482	8,766,203	5,470,354

TTP OR ACTION 8 Member	<p>TTP No. 8: Use “hack and leak” operation (which may or may not include doctored content)</p> <p>We have provided data on the CIO networks that we have disrupted in the reporting period under TTP No. 6. We have also provided data on violations of our Edited Media and AI-Generated Content (AIGC) policy under TTP No. 7. Our hack and leak policy was launched in H1 2024, but we do not have meaningful metrics under this policy to report for H1.</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 reporting 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 reporting period under TTP No. 6.</p>
-------------------------	--

TTP OR ACTION 11	<p>TTP No. 11. Non-transparent compensated messages or promotions by influencers</p> <p>Methodology of data measurement: We are unable to provide this metric due to insufficient data available for the reporting period.</p>			
	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4
	Number of actions taken by type			
Member States				
List actions per member states (see example table above)				



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 reporting 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 collaborated as part of the Integrity of Services working group to set up the first list of TTPs. We continue to provide updates on observed TTPs through our monthly CIO transparency reporting , including observations on novel and emerging tradecraft.



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.	
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"> • Building on our AI-generated content label for creators, and implementation of C2PA Content Credentials, we completed our AIGC media literacy campaign series in Mexico and the UK. These campaigns in Brazil, Germany, France, Mexico and the UK, which ran across H2 2024 and H1 2025, were developed with guidance from expert organisations like Mediawise and WITNESS to teach our community how to spot and label AI generated content. They reached more than 90M users globally, including more than 27M in Mexico and 10M in the UK. • Continued to join industry partners as a party to the “Tech Accord to Combat Deceptive Use of AI in 2024 Elections” which is a joint commitment to combat the deceptive use of AI in elections. • We continue to participate in relevant working groups, such as the Generative AI working group, which commenced 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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 15.1	



<p>QRE 15.1.1</p>	<p>Our Edited Media and AI-Generated Content (AIGC) policy includes commonly used and easily understood language when referring to AIGC, and outlines our existing prohibitions on AIGC showing fake authoritative sources or crisis events, or falsely showing public figures in certain contexts, including being bullied, making an endorsement, or being endorsed. As AI evolves, we continue to invest in combating harmful AIGC by evolving our proactive detection models, consulting with experts, and partnering with peers on shared solutions.</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 toggle 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 also automatically label content made with TikTok effects if they use AI. TikTok may automatically apply the “AI-generated” label to content we identify as completely generated or significantly edited with AI. This may happen when a creator uses TikTok AI effects or uploads AI-generated content that has Content Credentials attached, a technology from the Coalition for Content Provenance and Authenticity (C2PA). Content Credentials attach metadata to content that we can use to recognize and label AIGC instantly. Once content is labeled as AI-generated with an auto-label, users are unable to remove the label from the post.</p> <p>We do not allow:</p> <ul style="list-style-type: none"> • AIGC that shows the likeness of young people or realistic-appearing people under the age of 18 that poses a risk of sexualisation, bullying or privacy concerns, including those related to personally identifiable information or likeness to private individuals. • AIGC that shows the likeness of adult private figures, if we become aware it was used without their permission. • Misleading AIGC or edited media that falsely shows: <ul style="list-style-type: none"> ◦ Content made to seem as if it comes from an authoritative source, such as a reputable news organisation ◦ A crisis event, such as a conflict or natural disaster. ◦ A public figure who is: <ul style="list-style-type: none"> ■ being degraded or harassed, or engaging in criminal or antisocial behaviour.
--------------------------	---



	<ul style="list-style-type: none"> ■ taking a position on a political issue, commercial product, or a matter of public importance (such as an election). ■ being politically endorsed or condemned by an individual or group.
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 also proud to be a launch partner of the Partnership on AI's Responsible Practices for Synthetic Media.</p>

IV. Integrity of Services	
Commitment 16	
<p>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.</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].	Actively engaged with the Crisis Response working group, sharing insights and learnings about relevant areas, including CIOs.



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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 16.1	



QRE 16.1.1	<p>Central to our strategy for identifying and removing CIO on our platforms is working with our stakeholders, including civil society and 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 swiftly implement necessary actions in alignment with our policies.</p> <p>To provide more regular and detailed updates about the CIO we disrupt, we have introduced a new dedicated Transparency Report on covert influence operations, which is available in TikTok's Transparency Centre. In this report, we have also added new information about operations that we have previously removed and that have attempted to return to our platform with new accounts. The insights and metrics in this report aim to inform industry peers and the research community.</p> <p>We share relevant insights and metrics within our quarterly transparency reports, which aim to inform industry peers and the research community. We also review relevant insights and metrics from other industry peers to cross-compare for any similar behaviour on TikTok.</p> <p>We continue to engage in the subgroups set up for insights sharing between signatories and the Commission. For example, we've continued to participate in cross-industry forums such as elections stress test sessions organized by the Commission in Germany and Romania.</p> <p>As we have detailed in other chapters to this report, we have robust monetisation integrity policies in place and have established joint operating procedures between specialist CIO investigations teams and monetisation integrity teams to work on joint investigations of CIOs involving monetised products.</p>		
SLI 16.1.1 Numbers of actions as a result of information sharing	N/A		
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.	
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

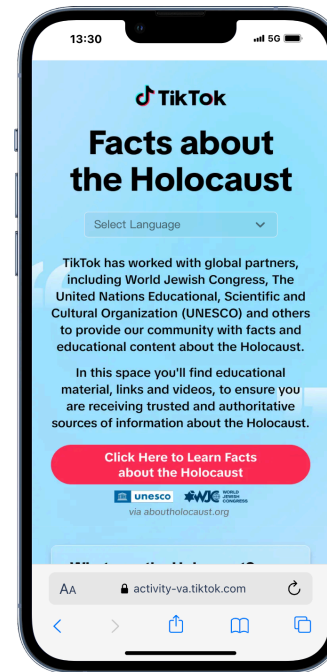


If yes, list these implementation measures here [short bullet points].

- Rolled out three new ongoing general media literacy and critical thinking skills campaigns in the EU in collaboration with our fact-checking and media literacy partners:
 - Germany: Deutsche Presse-Agentur (dpa)
 - Romania: Funky Citizens, Digi Media, and Libertatea
 - Poland: Demagog, FakeNews.pl, Radio Zet, and [Orientuj.sie](https://orientuj.sie)

This brings the number of general media literacy and critical thinking skills campaigns in Europe to 14 (Denmark, Finland, France, Georgia, Germany, Ireland, Italy, Romania, Spain, Sweden, Moldova, Netherlands, Poland and Portugal).

- We ran 9 temporary media literacy election integrity campaigns in advance of regional elections, most in collaboration with our fact-checking and media literacy partners:
 - 7 in the EU
 - Croatia (local election): Faktograf
 - Croatia (presidential election): Faktograf
 - Germany: Deutsche Presse-Agentur (dpa)
 - Latvia: Lead Stories
 - Poland: Demagog.pl and FakeNews.pl
 - Portugal: Poligrafo
 - Romania: Funky Citizens
 - 2 in wider European/regionally relevant countries
 - Albania: Internews Kosova (Kallxo)
 - Greenland: Logically Facts
- During the reporting period, we ran 7 Election Speaker Series sessions, 3 in EU Member States and 4 in Albania, Belarus, Greenland, and Kosovo.
 1. Albania: Internews Kosova (Kallxo)
 2. Belarus: Belarusian Investigative Center
 3. Germany: Deutsche Presse-Agentur (dpa)
 4. Greenland: Logically Facts
 5. Kosovo: Internews Kosova (Kallxo)
 6. Poland: Demagog
 7. Portugal: Poligrafo
- Launched a revamped version of our [Holocaust Education Campaign](#) providing a dedicated hub within the app, in partnership with the World Jewish Congress and UNESCO with new videos from our partners designed to inform our community about the Holocaust. This includes first-hand witness accounts from Holocaust [survivors](#), videos of users [visiting](#) Holocaust memorial sites, testimonials from curators sharing [stories](#) about Holocaust victims, and more. Our community can access the hub through TikTok searches related to the Holocaust and on relevant videos.



- Launched 2 new temporary search guides to provide users with guidance about interacting with sensitive content, and authoritative information sources, when events are unfolding rapidly.
 - Italy and Portugal: Pope Francis, Health Status, 14 Mar 2025 - 12 May 2025
 - Ireland and UK: Ballymena Riots, 13 Jun 2025 - 24 June 2025
- Launched a new temporary in-app natural disaster **media literacy search guide** for the Reunion Cyclone Garance between 4 March and 4 April 2025 and continued our temporary search guide for the Mayotte Cyclone until 14 Feb 2025. These search guides link to TikTok's Safety Center [tragic events support guide](#) and authoritative [third party](#) information about aid and relief support.
- Continued our 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 elections, the Israel-Hamas Conflict, Climate Change, Holocaust Education, Mpox, and the War in Ukraine.



	<ul style="list-style-type: none"> Expanded the scope of Verified for Climate—a joint initiative of the UN and social impact agency Purpose—to the UK and Indonesia, with operations in Brazil also scaled up. Now active in Brazil, Indonesia, UAE, UK, and Spain, our network of Verified Champions grew from 35 to over 90 trusted messengers. TikTok users shared more than 108,000 responses in H1 2025 to a short survey in TikTok after watching Verified Champion's: <ul style="list-style-type: none"> 70% learned something new about tackling climate challenges 73% feel more confident their communities can make a difference on climate issues 83% expressed increased support for renewable energy adoption Continued to support mental well-being awareness and literacy and to combat misinformation with reliable content through the WHO's Fides network, a diverse community of trusted healthcare professionals and content creators in Brazil, France, Indonesia, Japan, Korea, UK, and US. Completed our AIGC media literacy campaign series in Mexico and the UK. These campaigns in Brazil, Germany, France, Mexico and the UK, which ran across H2 2024 and H1 2025, were developed with guidance from expert organisations like Mediawise and WITNESS to teach our community how to spot and label AI generated content. They reached more than 90M users globally, including more than 27M in Mexico and 10M in the UK. Brought greater transparency about our systems and our integrity and authenticity efforts to our community by sharing regular insights and updates. In H1 2025, we launched a new: <ul style="list-style-type: none"> Transparency Center Global Elections Hub , including dedicated coverage of elections across Europe, the Middle East, and Africa. The Hub outlines our policies, product features, and moderation practices that help protect platform integrity during elections. Throughout this reporting period, we regularly updated the Hub with information on our safety efforts in markets with active elections, including Croatia, Kosovo, Germany, Romania, Portugal, and Poland. Safety Center user friendly guide on Making your feed For You. Invested in training and development for our human moderation teams. In H1 2025, all moderators received Fairness Training, a learning journey for addressing unconscious bias, and received ongoing Policy Training (1-4 hours of learning per week).
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]	N/A



<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<p>N/A</p>
<p>Measure 17.1</p>	
<p>QRE 17.1.1</p>	<p>In addition to actioning content that violates our Integrity and Authenticity policies, we continue to dedicate resources to: expanding our in-app measures that show users additional context on certain content (e.g., natural disasters and rapidly unfolding events); 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, we work with 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>We deploy a combination of in-app user intervention tools on topical issues such as elections , the Israel-Hamas Conflict, Holocaust Education, Mpox and the War in Ukraine.</p> <p>Video notice tags.</p> <p>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</i> [the topic]”. Users will be directed to an in-app guide, or reliable third party resource, as appropriate.</p>
<p>SLI 17.1.1</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>



	Total count of the tool's impressions	Interactions/ engagement with the tool	Other relevant metrics
	Number of impressions of the State-Controlled Media label	Number of clicks of the State-Controlled Media label	Click through rate of the State-Controlled Media label
Member States			
Austria	4,862,585	12,795	0.26%
Belgium	5,649,136	12,699	0.22%
Bulgaria	12,668,964	17,981	0.14%
Croatia	1,411,654	3,255	0.23%
Cyprus	941,853	1,850	0.20%
Czech Republic	23,121,314	28,454	0.12%
Denmark	3,386,494	10,044	0.30%
Estonia	2,098,586	4,169	0.20%
Finland	5,540,459	15,711	0.28%
France	23,552,580	41,708	0.18%
Germany	38,914,554	80,457	0.21%
Greece	4,299,200	15,000	0.35%
Hungary	34,538,866	21,238	0.06%
Ireland	3,667,705	7,912	0.22%
Italy	10,398,983	20,928	0.20%
Latvia	4,490,912	6,754	0.15%



Lithuania	3,548,967	7,957	0.22%
Luxembourg	467,744	989	0.21%
Malta	505,054	792	0.16%
Netherlands	14,196,897	35,399	0.25%
Poland	16,907,780	25,307	0.15%
Portugal	1,600,828	5,724	0.36%
Romania	34,425,296	47,348	0.14%
Slovakia	2,319,961	4,505	0.19%
Slovenia	1,039,188	2,167	0.21%
Spain	8,630,628	20,853	0.24%
Sweden	8,841,573	19,572	0.22%
Iceland	283,725	767	0.27%
Liechtenstein	43,166	75	0.17%
Norway	3,993,944	11,830	0.30%
Total EU	272,027,761	471,568	0.17%
Total EEA	276,348,596	484,240	0.18%

	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	11,841,886	36,538	0.31%
Belgium	7,726,879	29,679	0.38%
Bulgaria	1,900,093	10,945	0.58%
Croatia	2,060,663	8,943	0.43%
Cyprus	768,867	3,667	0.48%
Czech Republic	10,483,057	50,566	0.48%
Denmark	4,618,184	21,297	0.46%
Estonia	1,065,120	4,463	0.42%
Finland	8,294,809	30,022	0.36%
France	4,986,123	24,121	0.48%
Germany	104,872,400	278,958	0.27%
Greece	6,146,220	33,808	0.55%
Hungary	8,917,586	39,829	0.45%
Ireland	7,878,179	25,203	0.32%
Italy	6,112,796	25,852	0.42%
Latvia	1,160,441	4,639	0.40%
Lithuania	1,983,413	8,286	0.42%
Luxembourg	594,175	2,737	0.46%



Malta	511,099	1,555	0.30%
Netherlands	25,992,023	87,782	0.34%
Poland	56,430,318	184,865	0.33%
Portugal	4,875,624	23,827	0.49%
Romania	9,619,233	43,468	0.45%
Slovakia	2,323,018	10,422	0.45%
Slovenia	1,600,848	5,992	0.37%
Spain	19,547,025	88,547	0.45%
Sweden	11,793,010	59,461	0.50%
Iceland	615,803	2,484	0.40%
Liechtenstein	36,861	150	0.41%
Norway	6,731,013	31,942	0.47%
Total EU	324,103,089	1,145,472	0.35%
Total EEA	331,486,766	1,180,048	0.36%
	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	181,793	319	0.18%
Belgium	317,185	843	0.27%



Bulgaria	116,312	308	0.26%
Croatia	41,947	110	0.26%
Cyprus	19,130	29	0.15%
Czech Republic	127,675	425	0.33%
Denmark	46,773	131	0.28%
Estonia	20,787	39	0.19%
Finland	165,565	461	0.28%
France	3,786,548	9,788	0.26%
Germany	1,863,039	3,192	0.17%
Greece	107,619	279	0.26%
Hungary	115,889	402	0.35%
Ireland	331,243	439	0.13%
Italy	549,350	1,432	0.26%
Latvia	27,973	57	0.20%
Lithuania	52,298	133	0.25%
Luxembourg	14,854	23	0.15%
Malta	5,217	8	0.15%
Netherlands	255,494	568	0.22%
Poland	390,629	910	0.23%



Portugal	22,688	77	0.34%
Romania	215,427	557	0.26%
Slovakia	16,890	35	0.21%
Slovenia	19,780	28	0.14%
Spain	678,054	1,249	0.18%
Sweden	220,107	507	0.23%
Iceland	5,936	15	0.25%
Liechtenstein	458	1	0.22%
Norway	78,733	209	0.27%
Total EU	9,710,266	22,349	0.23%
Total EEA	9,795,393	22,574	0.23%
	Number of impressions of topic covered by video Intervention (Election)	Number of clicks by video Intervention (Election)	Click Through Rate by video Intervention (Election)
Member States			
Austria	—	—	—
Belgium	—	—	—
Bulgaria	—	—	—
Croatia	20,159,138	36,566	0.18%
Cyprus	—	—	—



Czech Republic	—	—	—
Denmark	—	—	—
Estonia	—	—	—
Finland	—	—	—
France	—	—	—
Germany	1,448,460,645	2,657,579	0.18%
Greece	—	—	—
Hungary	—	—	—
Ireland	—	—	—
Italy	—	—	—
Latvia	—	—	—
Lithuania	—	—	—
Luxembourg	—	—	—
Malta	—	—	—
Netherlands	—	—	—
Poland	2,037,979,838	2,643,385	0.13%
Portugal	—	—	—
Romania	1,818,730,718	2,518,345	0.14%
Slovakia	—	—	—

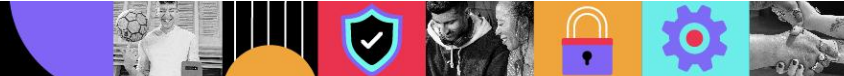


Slovenia	—	—	—
Spain	—	—	—
Sweden	—	—	—
Iceland	—	—	—
Liechtenstein	—	—	—
Norway	—	—	—
Total EU	5,325,330,339	7,855,875	0.15%
Total EEA	5,325,330,339	7,855,875	0.15%

	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	20,822	2,718	13.05%
Belgium	35,981	4,561	12.68%
Bulgaria	7,781	1,087	13.97%
Croatia	12,821	1,519	11.85%
Cyprus	2,139	238	11.13%
Czech Republic	13,713	1,787	13.03%
Denmark	9,891	1,096	11.08%



Estonia	2,764	255	9.23%
Finland	15,974	1,257	7.87%
France	332,240	39,478	11.88%
Germany	190,243	24,202	12.72%
Greece	13,311	1,289	9.68%
Hungary	13,136	1,789	13.62%
Ireland	16,337	1,215	7.44%
Italy	53,592	6,838	12.76%
Latvia	3,253	346	10.64%
Lithuania	5,712	626	10.96%
Luxembourg	2,973	401	13.49%
Malta	1,158	103	8.89%
Netherlands	41,715	4,354	10.44%
Poland	558	74	13.26%
Portugal	11,758	1,296	11.02%
Romania	23,173	2,811	12.13%
Slovakia	6,081	727	11.96%
Slovenia	7,481	907	12.12%
Spain	390,281	40,708	10.43%



Sweden	29,254	2,698	9.22%
Iceland	1,480	119	8.04%
Liechtenstein	107	12	11.21%
Norway	15,292	1,628	10.65%
Total EU	1,264,142	144,380	11.42%
Total EEA	1,281,021	146,139	11.41%
	Number of impressions of Search interventions (Mpox)	Number of clicks of Search interventions (Mpox)	Click Through Rate of Search interventions (Mpox)
Member States			
Austria	8,900	33	0.37%
Belgium	9,662	25	0.26%
Bulgaria	3,487	25	0.72%
Croatia	3,384	22	0.65%
Cyprus	808	4	0.50%
Czech Republic	5,442	25	0.46%
Denmark	2,722	18	0.66%
Estonia	1,204	11	0.91%
Finland	4,950	31	0.63%
France	61,103	113	0.18%
Germany	79,677	150	0.19%



Greece	6,438	53	0.82%
Hungary	5,138	24	0.47%
Ireland	6,930	15	0.22%
Italy	27,697	164	0.59%
Latvia	1,507	7	0.46%
Lithuania	3,446	26	0.75%
Luxembourg	794	7	0.88%
Malta	470	3	0.64%
Netherlands	22,926	83	0.36%
Poland	20,174	118	0.58%
Portugal	21,763	38	0.17%
Romania	17,002	52	0.31%
Slovakia	3,196	17	0.53%
Slovenia	1,082	7	0.65%
Spain	18,000	45	0.25%
Sweden	9,420	46	0.49%
Iceland	224	3	1.34%
Liechtenstein	290	0	0.00%
Norway	8,176	35	0.43%



Total EU	347,322	1,162	0.33%
Total EEA	356,012	1,200	0.34%

	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	430,052	842	0.20%
Belgium	337,921	583	0.17%
Bulgaria	97,003	228	0.24%
Croatia	117,710	188	0.16%
Cyprus	24,190	50	0.21%
Czech Republic	181,165	289	0.16%
Denmark	217,306	354	0.16%
Estonia	31,313	75	0.24%
Finland	269,574	543	0.20%
France	1,481,384	1,259	0.08%
Germany	4,254,490	5,870	0.14%
Greece	214,336	563	0.26%
Hungary	239,657	430	0.18%
Ireland	333,927	254	0.08%



Italy	856,374	1,340	0.16%
Latvia	41,234	79	0.19%
Lithuania	95,481	203	0.21%
Luxembourg	27,614	75	0.27%
Malta	13,395	21	0.16%
Netherlands	557,896	858	0.15%
Poland	782,163	1,421	0.18%
Portugal	178,635	236	0.13%
Romania	252,472	397	0.16%
Slovakia	73,321	122	0.17%
Slovenia	39,189	69	0.18%
Spain	810,034	680	0.08%
Sweden	794,502	1,336	0.17%
Iceland	10,254	29	0.28%
Liechtenstein	958	1	0.10%
Norway	361,902	547	0.15%
Total EU	12,752,338	18,365	0.14%
Total EEA	13,125,452	18,942	0.14%



	Number of impressions of Search interventions (Election)	Number of clicks of Search interventions (Election)	Click Through Rate of Search interventions (Election)
Member States			
Austria	—	—	—
Belgium	—	—	—
Bulgaria	—	—	—
Croatia	410,757	1,477	0.36%
Cyprus	—	—	—
Czech Republic	—	—	—
Denmark	—	—	—
Estonia	—	—	—
Finland	168,699	462	0.27%
France	—	—	—
Germany	712,652	711	0.10%
Greece	—	—	—
Hungary	—	—	—
Ireland	—	—	—
Italy	—	—	—
Latvia	581,154	1,955	0.34%
Lithuania	—	—	—



Luxembourg	—	—	—
Malta	—	—	—
Netherlands	—	—	—
Poland	90,499,754	159,793	0.18%
Portugal	—	—	—
Romania	23,322,577	49,361	0.21%
Slovakia	—	—	—
Slovenia	—	—	—
Spain	—	—	—
Sweden	—	—	—
Iceland	—	—	—
Liechtenstein	—	—	—
Norway	—	—	—
Total EU	115,695,593	213,759	0.18%
Total EEA	115,695,593	213,759	0.18%

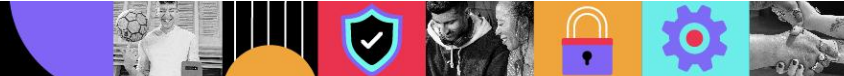
	Number of impressions of Public service announcements (Holocaust Misinformation/Denial)		
Member States			



Austria	19		
Belgium	62		
Bulgaria	19		
Croatia	6		
Cyprus	1		
Czech Republic	272		
Denmark	13		
Estonia	16		
Finland	67		
France	777		
Germany	466		
Greece	12		
Hungary	12		
Ireland	17		
Italy	52		
Latvia	40		
Lithuania	19		
Luxembourg	5		
Malta	0		



Netherlands	113		
Poland	112		
Portugal	6		
Romania	26		
Slovakia	5		
Slovenia	2		
Spain	36		
Sweden	51		
Iceland	0		
Liechtenstein	0		
Norway	32		
Total EU	2,226		
Total EEA	2,258		
	Number of impressions of Public service announcements (Mpox)		
Member States			
Austria	0		
Belgium	1		
Bulgaria	0		
Croatia	0		



Cyprus	0		
Czech Republic	4		
Denmark	0		
Estonia	0		
Finland	0		
France	3		
Germany	3		
Greece	0		
Hungary	1		
Ireland	2		
Italy	0		
Latvia	2		
Lithuania	0		
Luxembourg	0		
Malta	0		
Netherlands	3		
Poland	0		
Portugal	0		
Romania	1		



Slovakia	0		
Slovenia	0		
Spain	4		
Sweden	3		
Iceland	0		
Liechtenstein	0		
Norway	0		
Total EU	27		
Total EEA	27		

Measure 17.2	
--------------	--



QRE 17.2.1

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.

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).

(I) Promoting election integrity. As well as the election integrity pages on TikTok's [Safety Center](#) and [Transparency Center](#), and the new dedicated [Global Elections Hub](#), which provides an overview of our overall approach to protecting TikTok through the elections, including the most relevant policies that we use to protect the platform during elections, our media literacy features, and the continuous updates we make to support our community in real-time. Along with the hub, we launched media literacy campaigns in advance of several elections in the EU and wider Europe.

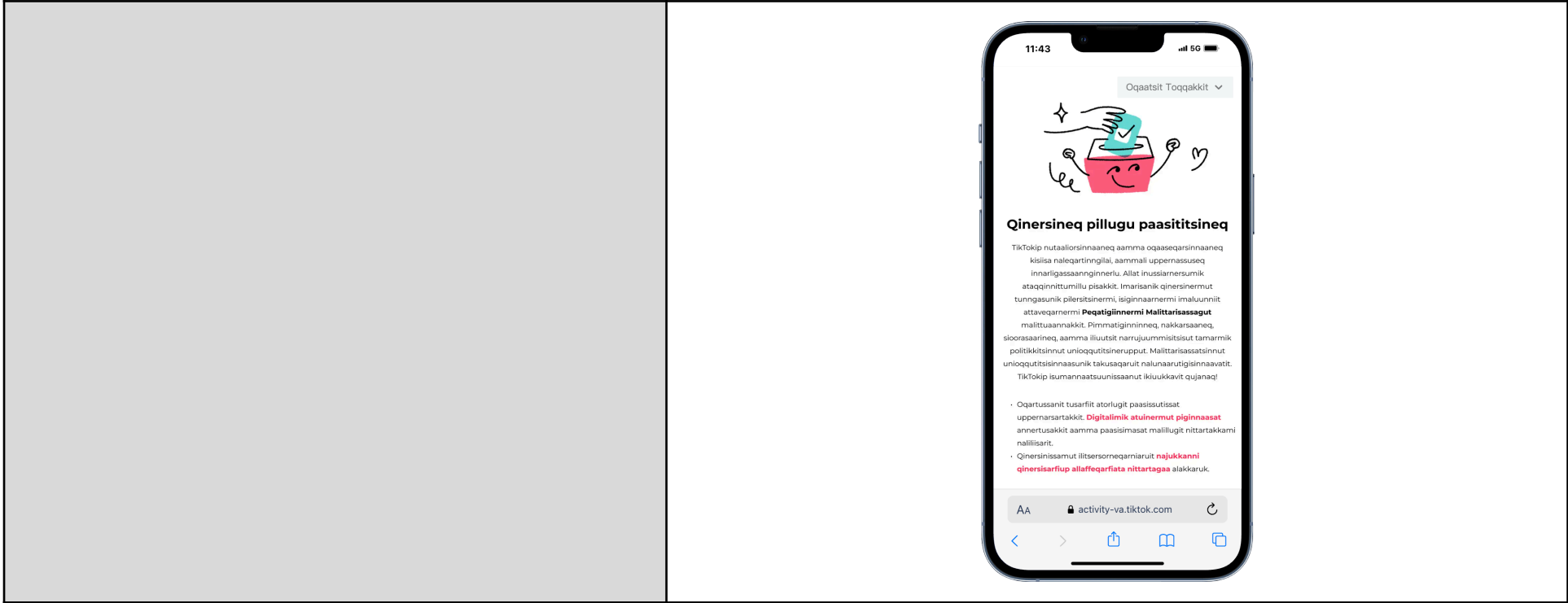
- **Croatia Presidential Election 2024:** From 6 Dec 2024 - 14 Jan 2025, we launched an in-app [Election Centre](#) to provide users with up-to-date information about the 2024 Croatia presidential election. The centre contained a section about spotting misinformation, which included videos created in partnership with the fact-checking organisation [Faktograf](#).



- **German Federal Election 20254:** From 16 Dec 2024 - 3 Mar 2025, we launched an in-app [Election Centre](#) to provide users with up-to-date information about the 2025 German federal election. The centre contained a section about spotting misinformation, which included videos created in partnership with the fact-checking organisation [Deutsche Presse-Agentur \(dpa\)](#).



- Greenland General Election 2025:** From 18 Feb 2025 - 12 Mar 2025, we launched an in-app [Search Guide and Details Page](#) to provide users with up-to-date information about the Greenland general election. The page contained a section about following our Community Guidelines, with a link to our Danish fact-checking partner, [Logically Facts](#) for digital literacy resources.





- Finland Local and Municipal Elections 2025:** From 4 Apr 2025 - 14 Apr 2025, we launched an in-app Search Guide and Details Page to provide users with up-to-date information about the Finnish elections and a link to a [government website](#) with election information. The page contained a section about following our Community Guidelines, with a link to the [Finnish National Agency for Education \(EDUFI\)](#) for digital literacy resources.



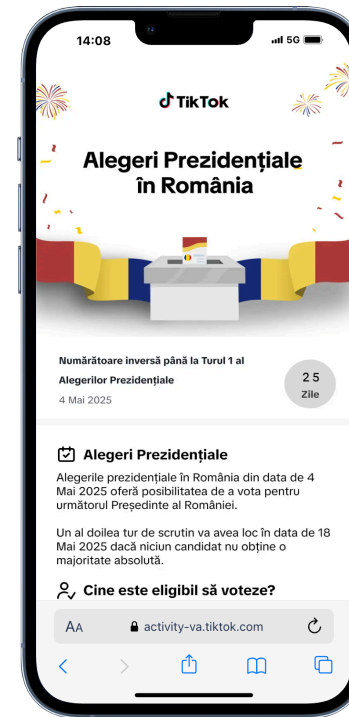
Tietoa vaaleista

TikTok arvostaa luovuutta ja ilmaisua, mutta myös aitoutta ja rehellisyyttä. Kohtele muita ystävällisesti ja kunnioittavasti. Noudata aina

Yhteisön suuntaviivat, kun luot ja katsot vaaleihin liittyvää sisältöä tai olet vuorovaikutuksessa sen kanssa. Käytännötämme kieltävät kiusaamisen, häirinnän, uhkailun ja kaikenlaisen loukkaavan käytöksen. Jos näet jotain, jonka uskot rikkovan sääntöjämme, voit ilmoittaa siitä. Kiitos, että autat meitä pitämään TikTokin turvallisena!

- Tarkista tiedot virallisista lähteistä. Kehitä **digilukutaitoa** ja tee tietopohjaisia päätöksiä verkossa.
- Äänestysohjeita löydät **oikeusministeriön vaalisivuilta**.

- **Romania Presidential Election 2025:** From 11 Apr 2025 - 23 May 2025, we launched an in-app [Election Centre](#) to provide users with up-to-date information about the 2025 Romanian elections. The centre contained a section about spotting misinformation, which included videos created in partnership with the fact-checking organisation [Funky Citizens](#) and media agencies [Digi Media](#) and [Libertatea](#).



- **Albania General Election 2025:** From 14 Apr 2025 - 12 May 2025, we launched an in-app [Election Centre](#) to provide users with up-to-date information about the 2025 Albanian elections. The centre contained a section about spotting misinformation, which included videos created in partnership with our fact-checking partner [Kallxo](#).



- Croatia Local Elections 2025:** From 17 Apr 2025 - 5 Jun 2025, we launched an in-app Search Guide and Details Page to provide users with up-to-date information about the Croatian local election. The page contained a section about following our Community Guidelines, with a link to our Croatia fact-checking partner, [Faktograf](#) for digital literacy resources.



vodafone UK 15:55



Svijest o izborima

TikTok cijeni kreativnost i izražavanje, ali i autentičnost i integritet. Odnosi se prema drugima s ljubaznošću i poštovanjem. Uvijek se pridržavaj dokumenta **Community Guidelines** pri izradi, gledanju ili interakciji sa sadržajem vezanim uz izbore. Maltretiranje, zlostavljanje, prijetnje i svi oblici nasilnog ponašanja protivne se našim pravilima. Vidiš li nešto što misliš da bi moglo kršiti naše smjernice, možeš to prijaviti. Hvala ti što pomažeš očuvati TikTok sigurnim!

- Koristi se kompetentnim izvorima za provjeru informacija. Razvijaj **vještine digitalne pismenosti** i donosi upućene prosudbe na internetu.
- Posjeti **mrežno mjesto lokalnog biračkog ureda** za smjernice u vezi glasanja.

Pošalji povratne informacije

- **Portugal Legislative Election 2025:** From 18 Apr 2025 to 2 June 2025, (ongoing at date of publication), we launched an in-app [Election Centre](#) to provide users with up-to-date information about the 2025 Portuguese election. The centre contained a section about spotting misinformation, which included videos created in partnership with our fact-checking partner Poligrafo.



- **Poland Presidential Election 2025:** From 18 Apr 2025 - 6 Jun 2025, we launched an in-app [Election Centre](#) to provide users with up-to-date information about the 2025 Polish election. The centre contained a section about spotting misinformation, which included videos created in partnership with our fact-checking partner [Demagog](#), fact checker [FakeNews.pl](#), and media partners [Radio Zet](#) and [Orientuj.sie](#).



- **Latvia Local and Municipal Elections 2025:** From 9 May 2025 (ongoing at date of publication), we launched an in-app Search Guide and Details Page to provide users with up-to-date information about the Latvian elections. The page contained a section about following our Community Guidelines, with a link to our Croatia fact-checking partner, [Lead Stories](#) for digital literacy resources.



(II) Election Speaker Series. To further promote election integrity, and inform our approach to elections, we invited suitably qualified local and regional external experts to share their insights and market expertise with our internal teams. During this reporting period, we ran **7 Election Speaker Series sessions**, 3 in EU Member States, and 4 in Albania, Belarus, Greenland, and Kosovo.

1. Albania: Internews Kosova (Kallxo)
2. Belarus: Belarusian Investigative Center
3. Germany: dpa
4. Greenland: Logically Facts
5. Kosovo: Kallxo
6. Poland: Demagog.pl
7. Portugal: Poligrafo



(III) Media literacy (General). We rolled out 3 new ongoing **general media literacy and critical thinking skills campaigns** in the EU in collaboration with our fact-checking and media literacy partners:

- Germany: Deutsche Presse-Agentur (dpa)
- Romania: Funky Citizens, Digi Media, and Libertatea
- Poland: Demagog.pl, FakeNews.pl, Radio Zet, and [Orientuj.sie](https://orientuj.sie)

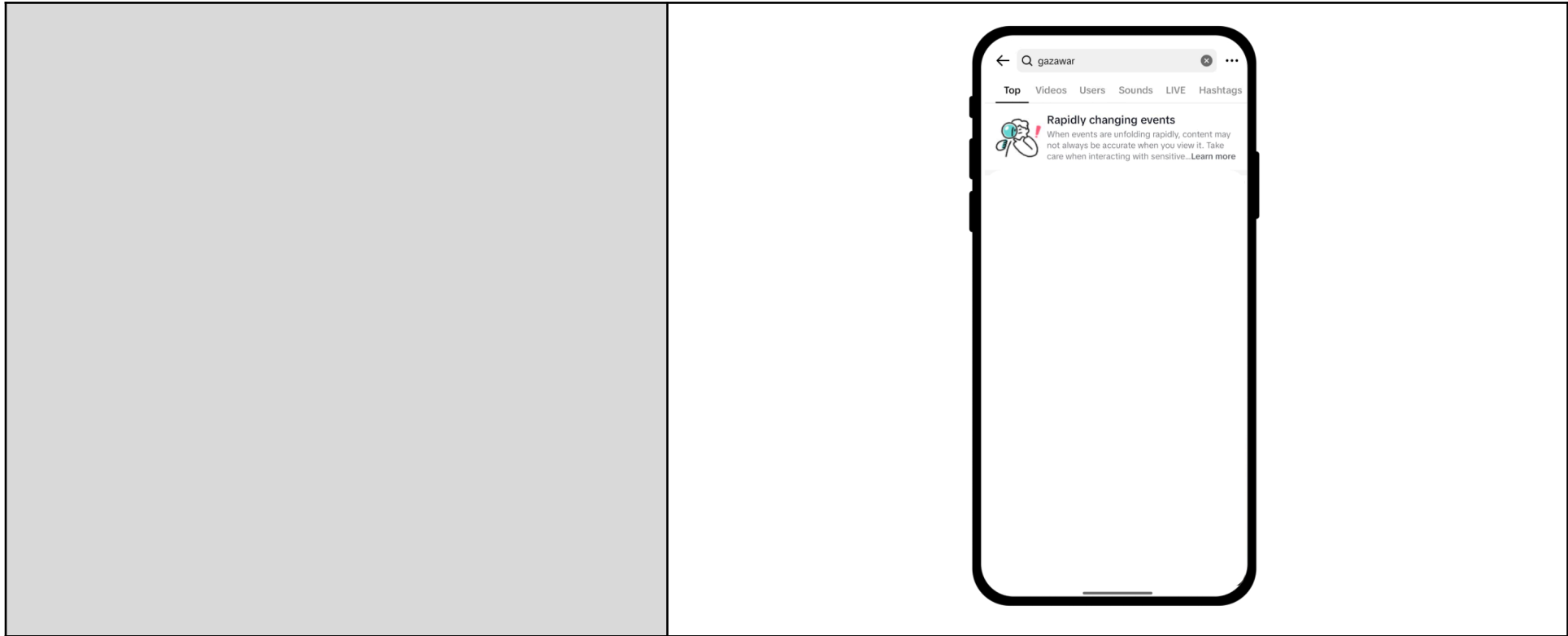
This brings the number of general media literacy and critical thinking skills campaigns in Europe to 14 (Denmark, Finland, France, Georgia, Germany, Ireland, Italy, Romania, Spain, Sweden, Moldova, Netherlands, Poland and Portugal).

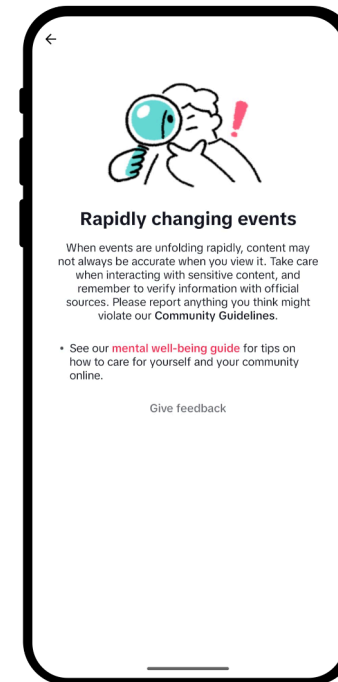
(IV) Media literacy (War in Ukraine). We continue to serve 17 localised media literacy campaigns specific to the war in Ukraine in: Ukraine, Romania, Slovakia, Hungary, Latvia, Estonia, Lithuania, Czechia, Poland, Croatia, Slovenia, Bulgaria, Germany, Austria, Bosnia, Montenegro, and Serbia.

- Partnered with Lead Stories: Ukraine, Romania, Slovakia, Hungary, Latvia, Estonia, Lithuania.
- Partnered with fakenews.pl: Poland.
- Partnered with Correctiv: Germany, Austria.

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 search interventions which are triggered when users search for neutral 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](#) is available in 23 official EU languages (plus Norwegian and Icelandic for EEA users). It redirects users looking for climate change-related content to authoritative information and encourages them to report any potential misinformation they see.



Member States	Total number of impressions of the H5 Page (Views generated between January 1 and July 31, 2025)	Number of impressions of the search intervention	Number of clicks on the search intervention	Click through rate of the search intervention
France (in partnership with AFP)	67,229	26,929,963	93,276	0.35%
Portugal (in partnership with Poligrafo)	11,717	5,912,394	24,653	0.42%
Denmark (in partnership with Logically Facts)	1,108	282,335	1,298	0.46%
The Netherlands (in partnership with Nieuwscheckers)	6,362	2,675,339	8,535	0.32%
Ireland (in partnership with The journal.ie)	1,533	541,877	2,771	0.51%
Finland (in partnership with Logically Facts)	757	169,420	1,480	0.87%
Sweden (in partnership with Logically Facts)	1,661	348,248	2,740	0.79%
Spain (in partnership with Maldita)	31,343	21,936,930	51,879	0.24%
Italy (in partnership with Facta)	2,474	777,747	3,706	0.48%
Austria (in partnership with Correctiv, joint campaign with Germany)	4,585	1,222,624	6,041	0.49%
Germany (in partnership with Correctiv, joint campaign with Austria)	27,334	12,978,052	36,952	0.28%

Bulgaria	1,286	393,344	2,070	0.53%
Croatia	1,350	598,599	2,401	0.40%
Czech Republic	2,231	1,215,910	4,116	0.34%
Slovenia	512	155,929	759	0.49%

Measure 17.3	
--------------	--



QRE 17.3.1

As documented in the TikTok Safety Center [Safety Partners](#) page and [TikTok's Advisory Councils](#), 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:

(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.

- Outside of our fact-checking program, we also collaborate with fact-checking organisations to develop a variety of media literacy campaigns. For example, during this reporting period, we worked with European fact-checkers on 9 temporary **media literacy election integrity campaigns**, in advance of regional elections, through our in-app Election Centers:
 - 7 in the EU
 - Croatia (local election): Faktograf
 - Croatia (presidential election): Faktograf
 - Germany: Deutsche Presse-Agentur (dpa)
 - Latvia: Lead Stories
 - Poland: Demagog and FakeNews.pl
 - Portugal: Poligrafo
 - Romania: Funky Citizens
 - 2 in wider European regionally relevant countries
 - Albania: Internews Kosova (Kallxo)
 - Greenland: Logically Facts
- **Election speaker series.** To further promote election integrity, and inform our approach to 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 the following organisations:
 1. Albania: Internews Kosova (Kallxo) Kallxo
 2. Belarus: Belarusian Investigative Center



	<ol style="list-style-type: none"> 3. Germany: Deutsche Presse-Agentur (dpa)DPA 4. Greenland: Logically Facts 5. Kosovo: Kallxo 6. Poland: Demagog 7. Portugal: Poligrafo <p>(II) War in Ukraine. We continue to run our media literacy campaigns about the war in Ukraine, developed in partnership with our media literacy partners Correctiv in Austria and Germany, Fakenews.pl in Poland and Lead Stories in Ukraine, Romania, Slovakia, Hungary, Latvia, Estonia, Lithuania. We also expanded this campaign to Serbia, Bosnia, Montenegro, Czechia, Croatia, Slovenia, Bulgaria.</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 improve the accuracy of, and overall coverage provided by, our machine learning detection models. • Began testing large language models (LLMs) to further support proactive moderation at scale. Because LLMs can comprehend human language and perform highly specific, complex tasks, we are better able to moderate nuanced areas like misinformation by extracting specific misinformation "claims" from videos for moderators to assess directly or route to our fact-checking partners. • Invested in training and development for our Trust and Safety team, including regular internal sessions dedicated to knowledge sharing and discussion about relevant issues



	<p>and trends and attending external events to share their expertise and support continued professional learning. For example:</p> <ul style="list-style-type: none"> ○ In the lead-up to certain elections, we invite suitably qualified external local/regional experts, as part of our Election Speaker Series. Sharing their market expertise with our internal teams provides us with insights to better understand areas that could potentially amount to election manipulation, and informs us about our approach to the upcoming election. During the reporting period, we ran 7 Election Speaker Series sessions, 3 in EU Member States, and 4 in Albania, Belarus, Greenland, and Kosovo. <ul style="list-style-type: none"> ▪ Albania: Internews Kosova (Kallxo) ▪ Belarus: Belarusian Investigative Center ▪ Germany: Deutsche Presse-Agentur (dpa) ▪ Greenland: Logically Facts ▪ Kosovo: Internews Kosova (Kallxo) ▪ Poland: Demagog ▪ Portugal: Poligrafo ○ In June 2025, 14 members of our Trust and Safety team (including leaders of our fact-checking program) attended GlobalFact12. In addition to a breakout session on Footnotes, TikTok hosted a networking event with more than 80 people from our partner organizations, including staff from fact checking partners, media literacy organizations, and Safety Advisory Councils. ○ TikTok teams and personnel also regularly participate in research-focused events. In H1 2025, we presented at the Political Tech Summit in Berlin (January), hosted Research Tools demos in Warsaw (April), Presented at GNET Annual Conference (May), hosted Research Tools demos in Prague (June), Presented at the Warsaw Women in Tech Summit (June), briefed a small group of Irish academic UCD (Dublin) researchers (June), and attended the ICWSM conference in Copenhagen (June). ● Continued to participate in, and co-chair, the working group on Elections.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	N/A



If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 18.1	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 18.1.1	N/A
QRE 18.1.2	N/A
QRE 18.1.3	N/A
SLI 18.1.1 - actions proving effectiveness of measures and policies	N/A
Measure 18.2	
QRE 18.2.1	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.



Our Terms of Service and Integrity and Authenticity policies under our Community Guidelines 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.

Specifically, our policies do not allow:

- **Misinformation**

- Misinformation that poses a risk to public safety or may induce panic about a crisis event or emergency, including using historical footage of a previous attack as if it were current, or incorrectly claiming a basic necessity (such as food or water) is no longer available in a particular location. Health misinformation, such as misleading statements about vaccines, inaccurate medical advice that discourages people from getting appropriate medical care for a life-threatening disease, or other misinformation which may cause negative health effects on an individual's life
- Climate change misinformation that undermines well-established scientific consensus, such as denying the existence of climate change or the factors that contribute to it.
- Conspiracy theories that name and attack individual people.
- Conspiracy theories that are violent or hateful, such as making a violent call to action, having links to previous violence, denying well-documented violent events, or causing prejudice towards a group with a protected attribute.

- **Civic and Election Integrity**

- Election misinformation, including:
 - How, when, and where to vote or register to vote;
 - Eligibility requirements of voters to participate in an election, and the qualifications for candidates to run for office;
 - Laws, processes, and procedures that govern the organisation and implementation of elections and other civic processes, such as referendums, ballot propositions, or censuses;
 - Final results or outcome of an election.

- **Edited Media and AI-Generated Content (AIGC)**

- The likeness of young people or realistic-appearing people under the age of 18.



- The likeness of adult private figures, if we become aware it was used without their permission.
- Misleading AIGC or edited media that falsely shows:
 - Content made to seem as if it comes from an authoritative source, such as a reputable news organisation;
 - A crisis event, such as a conflict or natural disaster.
- A public figure who is:
 - being degraded or harassed, or engaging in criminal or antisocial behaviour;
 - taking a position on a political issue, commercial product, or a matter of public importance (such as an election);
 - being politically endorsed or condemned by an individual or group.

- **Fake Engagement**

- Facilitating the trade or marketing of services that artificially increase engagement, such as selling followers or likes.
- Providing instructions on how to artificially increase engagement on TikTok.

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

- **Misinformation**

- 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"
- Moderate harm health misinformation, such as an unproven recommendation for how to treat a minor illness
- Repurposed media, such as showing a crowd at a music concert and suggesting it is a political protest
- Misrepresenting authoritative sources, such as selectively referencing certain scientific data to support a conclusion that is counter to the findings of the study
- Unverified claims related to an emergency or unfolding event
- Potential high-harm misinformation while it is undergoing a fact-checking review

- **Civic and Election Integrity**

- Unverified claims about an election, such as a premature claim that all ballots have been counted or tallied



- Statements that significantly misrepresent authoritative civic information, such as a false claim about the text of a parliamentary bill

- **Fake Engagement**

- Content that tricks or manipulates others as a way to increase gifts, or engagement metrics, such as "like-for-like" promises or other false incentives for engaging with content

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 Integrity and Authenticity policies. Individuals are notified of our decisions and can appeal them if they believe no violation has occurred. We also make clear in our Community Guidelines that we will temporarily or permanently ban accounts and/or users that are involved in serious or repeated violations, including violations of our Integrity and Authenticity policies.

We enforce our Community Guidelines policies, including our Integrity and Authenticity 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.

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



	<p>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 Community Guidelines, 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 Integrity and Authenticity policies 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 from users in the EEA that were recorded in H1 2025, fewer than 1 in per 10,000 views were of content identified and removed for violating our policies around harmful misinformation.</p>
SLI 18.2.1	<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, Civic and Election Integrity and Edited media and AIGC 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>We also updated the methodology on the number of videos made ineligible for the For You feed under our Misinformation policy.</p>



	Total no of violations	Metric 1: indicating the impact of the action taken	Total no of violations	Metric 1: indicating the 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 Misinformation policy.	
Member States				
Austria	2709	8,944,232	2,239	
Belgium	3853	11,135,550	4,174	
Bulgaria	3368	2,066,762	3,745	
Croatia	495	1,403,906	617	
Cyprus	441	2,756,634	428	
Czech Republic	4134	7,044,040	6,859	
Denmark	1267	1,953,383	1,145	
Estonia	305	62,493	587	
Finland	2451	34,614,594	1,226	
France	37041	74,342,227	47,842	



Germany	47342	169,217,792	43,591	
Greece	3094	35,470,406	3,203	
Hungary	1110	1,058,471	1,096	
Ireland	2850	2,913,140	3,088	
Italy	19673	80,387,048	39,252	
Latvia	412	4,092,236	516	
Lithuania	494	117,112	568	
Luxembourg	545	268,382	419	
Malta	504	27,622	468	
Netherlands	6426	10,368,861	9,720	
Poland	16929	33,132,517	14,452	
Portugal	2791	3,973,790	2,487	
Romania	24291	103,983,826	22,271	
Slovakia	3301	19,739,868	2,920	
Slovenia	2710	288,607	2,063	
Spain	16368	18,961,436	69,638	



Sweden	2742	4,494,654	2,396	
Iceland	73	29,170	150	
Liechtenstein	6	8	15	
Norway	1378	4,888,301	1,439	
Total EU	207,646	632,819,589	287,010	
Total EEA	209,103	637,737,068	288,614	
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	Number of videos removed because of violation of Synthetic and Manipulated Media	Number of views of videos removed because of violation of Synthetic and Manipulated Media
Member States				
Austria	953	1,047,899	585	1,786,611
Belgium	1,175	198,889	691	13,473,808
Bulgaria	371	110,715	261	16,896
Croatia	94	91,236	109	348,415
Cyprus	97	1,356	155	1,125,052
Czech Republic	660	478,219	356	3,259,466
Denmark	519	127	331	104,872



Estonia	36	40	89	262,860
Finland	517	9,986	142	1,719,209
France	5,863	4,248,076	4,373	47,569,470
Germany	15,556	11,619,658	5,389	50,209,813
Greece	1,152	6,312	648	2,412,820
Hungary	955	6,568	95	32,201
Ireland	714	43,459	250	80,522
Italy	6,762	5,503,370	2,510	6,572,802
Latvia	62	4,851	228	403,046
Lithuania	51	106,222	168	6,834,539
Luxembourg	57	125	37	102,103
Malta	28	1,897	31	1,462
Netherlands	1,250	1,785,149	988	2,127,647
Poland	1,728	9,960,972	655	6,968,424
Portugal	855	1,258,329	662	822,977
Romania	6,813	39,137,059	2,520	10,019,149
Slovakia	53	1,362	113	542,335
Slovenia	28	0	258	45,635
Spain	2,757	1,507,912	2,020	55,973,123



Sweden	1,201	977,060	549	402,955
Iceland	10	0	14	226
Liechtenstein	0	0	0	0
Norway	410	6,884	272	739,044
Total EU	50,307	78,106,848	24,213	213,218,212
Total EEA	50,727	78,113,732	24,499	213,957,482
Measure 18.3	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .			
QRE 18.3.1	N/A			

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"> At TikTok, we strive to bring more transparency to how we protect our platform. We continue to increase the reports we voluntarily publish, the depth of data we disclose, and the frequency with which we publish.



	<ul style="list-style-type: none"> • In H1 2025, we published updates to our transparency reports, including: <ul style="list-style-type: none"> ◦ Community Guidelines Enforcement Report (January-March 2025)July-September 2024) ◦ Covert Influence Operations Reports, where we shared information about the influence networks we disrupted from January-June 2025. ◦ Platform Security Report (January-March 2025) • We also worked to make it easier for people to independently study our data and platform. For example through: <ul style="list-style-type: none"> ◦ our Research Tools which empower over 900 research teams to independently study our platform. ◦ adding additional functionality to the Research API, including a compliance API (launched in June) that improves the data refresh process for researchers, helping to ensure that efforts to comply with our Terms of Service (ToS) do not impede researchers' ability to efficiently access data from TikTok's Research API. ◦ the downloadable data file in the Community Guidelines Enforcement Report offering access to aggregated data, including removal data by policy category, for the 50 markets with the highest volumes of removed content.
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 19.1	
QRE 19.1.1	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.



We make clear to users in our Terms of Service and Community Guidelines (and also provide more context in our Help Center [article](#) and Transparency Center [page](#), and Safety Center [guide](#)) 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 that violates our Community Guidelines, 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 content based on a combination of factors including:

- user interactions (e.g. content users like, share, comment on, and watch in full or skip, as well as accounts of followers that users follow back);
- Content information (e.g. sounds, hashtags, number of views, and the country the content was published); and
- User information (e.g. device settings, language preferences, location, time zone and day, and device types).

The main parameters help us make predictions on the content users are likely to be interested in. Different factors can play a larger or smaller role in what's recommended, and the importance – or weighting – of a factor can change over time. For many users, the time spent watching a specific video is generally weighted more heavily than other factors. 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.

Users can also access the “Why this video” feature, which allows them 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. **User preferences.**

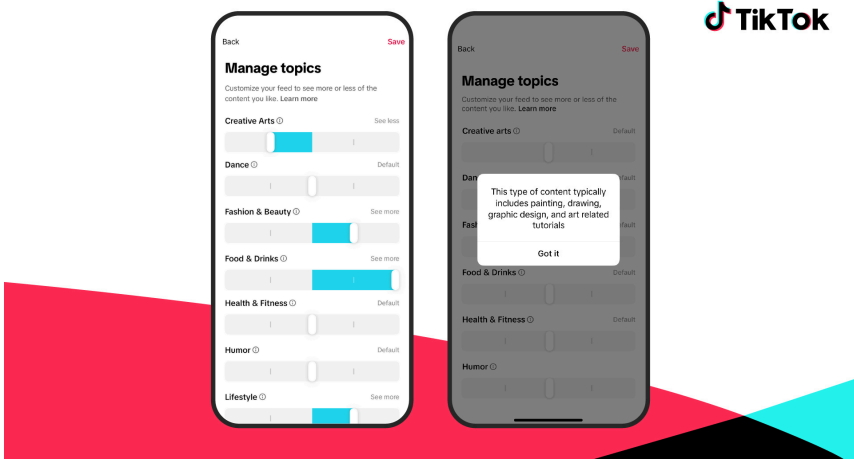


Together with the safeguards we build into our platform by design, we also empower our users to customise their experience to their preferences and comfort.

These include a number of features to help shape the content they see. For example, in the For You feed:

- Users can click on any video and select “not interested” to indicate that they do not want to see similar content.
- Users are able to automatically filter out specific words or hashtags from the content recommended to them(see [here](#)).
- Users are able to [refresh their For You feed](#) if they no longer feel like recommendations are relevant to them or are too similar. When the For You feed is refreshed, users view a number of new videos which include popular videos (e.g., they have a high view count or a high like rate). Their interaction with these new videos will inform future recommendations.
- Users can also personalise their "For You" page through our new **Manage Topics** feature (June 2025). This allows users to adjust the frequency of content they see related to particular topics. The settings don't eliminate topics entirely but can influence how often they're recommended as peoples' interests evolve over time. It adds to the many ways people shape their feed every day - including liking or sharing videos, searching for topics, or simply watching videos for longer.



	 <ul style="list-style-type: none"> As part of our obligations under the DSA (Article 38), we introduced non-personalized feeds on our platform, which provide our European users with an alternative to recommender systems. They are able to turn off personalisation so that feeds show non-personalised content. For example, the For You feed will instead show popular videos in their regions and internationally. See here.
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 users clicked “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> <p>The number for videos tagged with AIGC label includes both automatic and creator-generated labeling.</p>



	No of times users actively engaged with these settings	No of times users actively 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	Number of Videos tagged with AIGC label
Member States				
Austria	71,042	952,721	60,429	216,782
Belgium	109,999	1,428,998	109,438	310,518
Bulgaria	61,967	838,603	50,767	325,280
Croatia	36,204	396,069	25,456	62,728
Cyprus	15,655	199,425	17,429	105,231
Czech Republic	63,390	811,437	77,494	248,842
Denmark	47,704	585,499	32,565	103,602
Estonia	17,219	162,805	13,428	27,463
Finland	64,531	641,392	59,140	151,632
France	621,904	8,623,045	621,611	2,631,307
Germany	714,270	8,678,005	708,174	2,923,297
Greece	95,344	1,267,887	87,742	289,830
Hungary	60,520	1,056,004	34,031	242,598



Ireland	77,782	894,686	71,318	85,518
Italy	407,290	6,719,765	305,942	1,606,752
Latvia	25,337	298,797	29,270	73,324
Lithuania	31,173	339,592	27,527	74,036
Luxembourg	6,249	83,357	5,752	36,563
Malta	6,356	79,651	7,349	21,483
Netherlands	225,595	2,327,551	188,048	440,107
Poland	277,460	3,572,508	201,086	789,871
Portugal	97,779	1,208,681	73,846	354,910
Romania	149,926	2,827,115	268,322	685,318
Slovakia	26,822	363,060	16,471	112,814
Slovenia	13,155	174,113	17,172	26,794
Spain	475,525	7,262,327	430,715	1,837,668
Sweden	112,446	1,467,000	141,965	324,255
Iceland	6,330	60,021	3,572	9,200
Liechtenstein	180	3,636	295	211
Norway	65,219	733,515	53,304	118,623
Total EU	3,912,644	53,260,093	3,682,487	14,108,523
Total EEA	3,984,373	54,057,265	3,739,658	14,236,557



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]	TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document .
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]	N/A
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	N/A



Measure 20.2	
QRE 20.2.1	N/A

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"> • We ran 9 temporary media literacy election integrity campaigns in advance of regional elections, most in collaboration with our fact-checking and media literacy partners: <ul style="list-style-type: none"> ○ 7 in the EU <ul style="list-style-type: none"> ■ Croatia (local election): Faktograf ■ Croatia (presidential election): Faktograf ■ Germany: Deutsche Presse-Agentur (dpa) ■ Latvia: Lead Stories ■ Poland: Demagog and FakeNews.pl ■ Portugal: Poligrafo ■ Romania: Funky Citizens



	<ul style="list-style-type: none"> ○ 2 in wider European/regionally relevant countries <ul style="list-style-type: none"> ■ Albania: Internews Kosova (Kallxo) ■ Greenland: Logically Fact ● Continued our temporary in-app natural disaster media literacy search guide for the Mayotte Cyclone until 14 Feb 2025, and launched a new search guide for the Reunion Cyclone Garance between 4 March and 4 April 2025. These search guides link to TikTok's Safety Center tragic events support guide and authoritative third party information about aid and relief support. ● Continued our 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 elections, the Israel-Hamas Conflict, Climate Change, Holocaust Education, Mpox, and the War in Ukraine. ● We partner with fact checkers to assess the accuracy of content. Sometimes, our fact-checking partners determine that content cannot be confirmed or checks are inconclusive (especially during unfolding events). Where our fact-checking partners provide us with a rating that demonstrates the claim cannot yet be verified, we may use our unverified content label to inform viewers via a banner that a video contains unverified content, in an effort to raise user awareness about content credibility. ● Building on our new AI-generated content label for creators, and implementation of C2PA Content Credentials, we launched a number of media literacy campaigns with guidance from expert organisations like Mediawise and WITNESS, including in Brazil, Germany, France, Mexico and the UK, that teach our community how to spot and label AI-generated content. They reached more than 90M users globally, including more than 27M in Mexico and 10M in the UK.
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A



Measure 21.1	
QRE 21.1.1	<p>We currently have 12 IFCN accredited fact-checking partners across the EU, EEA, and wider Europe:</p> <ol style="list-style-type: none">1. Agence France-Presse (AFP)2. dpa Deutsche Presse-Agentur3. Demagog4. Facta5. Fact Check Georgia6. Faktograf7. Internews Kosova8. Lead Stories9. Newtral10. Poligrafo11. Reuters12. Teyit <p>These partners provide fact-checking coverage in 23 official EEA languages, including at least one official language of each EU Member States, plus Georgian, Russian, Turkish, and Ukrainian.</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-checking partners 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-checking partners 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-checking partners determine that content cannot be confirmed or checks are inconclusive (especially during unfolding events). Where our fact-checking partners provide us with a rating that demonstrates the claim cannot yet be verified, we may use our unverified content label to inform viewers [via a banner](#) that a video contains 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.
- **In-app tools related to specific topics:**
 - **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 France legislative elections in June 2024 included a search intervention and in-app [Election Centre](#). The centre contained a section about spotting misinformation, which included videos created in partnership with fact-checking organisation [Agence France-Presse \(AFP\)](#). In total, during the reporting period, we ran 14 temporary **media literacy election integrity campaigns** in advance of regional elections.
 - **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.
 - **Natural disasters:** Launched a new temporary in-app natural disaster media literacy search guide for the Reunion Cyclone Garance between 4 March and 4 April 2025 and continued our temporary search guide for the Mayotte Cyclone until 14 Feb 2025. These search guides link to TikTok's Safety Center [tragic events support guide](#) and authoritative [third party](#) information about aid and relief support.
- **User awareness of our fact-checking partnerships and labels.** We have created pages on our [Safety Center](#) and [Transparency Center](#) to raise users' awareness about our fact-checking program and labels and to support the work of our fact-checking partners.



SLI 21.1.1 - actions taken under measure 21.1	Methodology of data measurement: 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. 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	26.41%	18.55%	98.56%	80.73%	84.72%
Belgium	37.10%	28.82%	98.73%	77.11%	83.00%
Bulgaria	35.71%	45.82%	97.98%	55.05%	84.53%
Croatia	26.38%	25.45%	97.78%	72.32%	86.06%
Cyprus	34.36%	24.09%	97.28%	72.11%	80.27%



Czech Republic	28.55%	38.46%	98.26%	55.52%	94.22%
Denmark	31.84%	16.32%	98.90%	74.19%	86.90%
Estonia	30.33%	2.12%	98.69%	63.61%	80.00%
Finland	33.60%	27.42%	94.45%	70.50%	91.43%
France	37.30%	25.23%	99.10%	84.59%	91.27%
Germany	26.78%	27.90%	98.10%	79.18%	90.84%
Greece	30.79%	23.99%	98.97%	73.88%	89.04%
Hungary	32.45%	2.84%	97.39%	74.59%	92.61%
Ireland	29.28%	27.15%	97.54%	73.16%	80.88%
Italy	36.90%	28.38%	98.55%	78.93%	84.12%
Latvia	33.33%	17.22%	97.82%	83.01%	91.26%
Lithuania	29.57%	20.17%	99.19%	80.97%	87.04%
Luxembourg	28.85%	25.02%	89.36%	69.17%	92.11%
Malta	39.10%	50.81%	90.08%	70.63%	94.44%
Netherlands	29.46%	25.49%	99.16%	81.22%	87.35%
Poland	30.81%	37.85%	98.77%	65.49%	93.13%
Portugal	28.31%	27.48%	98.57%	84.09%	91.37%
Romania	35.42%	44.26%	96.03%	67.42%	86.84%
Slovakia	28.82%	62.64%	94.27%	67.80%	95.33%



Slovenia	25.24%	32.84%	93.76%	77.23%	98.71%
Spain	34.09%	30.23%	99.46%	87.87%	90.63%
Sweden	31.25%	15.83%	98.65%	78.99%	82.53%
Iceland	22.73%	8.01%	98.63%	89.04%	90.41%
Liechtenstein	11.76%	8.00%	100.00%	66.67%	66.67%
Norway	32.93%	16.73%	98.33%	69.09%	87.01%
Total EU	30.95%	27.42%	98.11%	76.94%	89.47%
Total EEA	30.95%	27.28%	98.11%	76.90%	89.45%
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		6.53%	99.06%	93.18%	92.13%
Belgium		8.79%	99.57%	95.91%	95.66%
Bulgaria		5.05%	99.73%	97.04%	97.84%
Croatia		4.83%	96.81%	87.23%	91.49%
Cyprus		5.30%	97.94%	88.66%	87.63%
Czech Republic		6.14%	99.70%	97.27%	97.73%



Denmark		6.69%	99.81%	98.27%	98.07%
Estonia		0.25%	100.00%	97.22%	97.22%
Finland		5.78%	99.81%	95.94%	98.84%
France		3.99%	99.52%	95.00%	95.77%
Germany		9.17%	98.25%	89.13%	91.11%
Greece		8.93%	99.91%	96.18%	98.70%
Hungary		2.44%	99.06%	89.01%	99.48%
Ireland		6.80%	99.30%	77.17%	98.04%
Italy		9.76%	99.42%	94.08%	92.75%
Latvia		2.59%	100.00%	95.16%	95.16%
Lithuania		2.08%	98.04%	96.08%	96.08%
Luxembourg		2.62%	100.00%	87.72%	87.72%
Malta		2.82%	100.00%	89.29%	89.29%
Netherlands		4.96%	99.04%	97.04%	97.12%
Poland		3.86%	97.34%	85.94%	84.66%
Portugal		8.42%	98.13%	92.28%	94.85%
Romania		12.41%	94.39%	80.65%	71.79%
Slovakia		1.01%	100.00%	92.45%	92.45%
Slovenia		0.34%	100.00%	100.00%	100.00%



Spain		5.09%	99.31%	92.75%	89.88%
Sweden		6.94%	99.67%	96.92%	96.84%
Iceland		1.10%	100.00%	100.00%	100.00%
Liechtenstein		0.00%	0.00%	0.00%	0.00%
Norway		4.98%	98.78%	93.41%	94.39%
Total EU		6.64%	98.29%	90.43%	90.17%
Total EEA		6.62%	98.30%	90.46%	90.21%
Member States		% video removals under Synthetic Media policy	% proactive video removals under Synthetic Media policy	% video removals before any views under Synthetic Media policy	% video removals within 24h under Synthetic Media policy
Austria		4.01%	96.75%	43.59%	45.30%
Belgium		5.17%	96.82%	19.68%	16.64%
Bulgaria		3.55%	99.23%	22.61%	24.14%
Croatia		5.60%	93.58%	22.02%	40.37%
Cyprus		8.47%	96.77%	30.32%	28.39%
Czech Republic		3.31%	94.94%	37.64%	57.58%
Denmark		4.26%	96.37%	30.21%	50.15%
Estonia		0.62%	98.88%	59.55%	68.54%



Finland		1.59%	97.89%	27.46%	41.55%
France		2.98%	96.16%	22.30%	23.12%
Germany		3.18%	93.75%	35.63%	44.09%
Greece		5.02%	96.45%	17.75%	27.78%
Hungary		0.24%	90.53%	32.63%	31.58%
Ireland		2.38%	98.00%	30.00%	30.00%
Italy		3.62%	96.61%	20.04%	13.75%
Latvia		9.53%	98.25%	64.04%	78.95%
Lithuania		6.86%	97.02%	59.52%	66.67%
Luxembourg		1.70%	91.89%	27.03%	27.03%
Malta		3.13%	100.00%	9.68%	25.81%
Netherlands		3.92%	95.85%	22.27%	33.60%
Poland		1.46%	94.35%	39.69%	46.26%
Portugal		6.52%	99.40%	25.68%	18.28%
Romania		4.59%	95.44%	32.38%	25.04%
Slovakia		2.14%	97.35%	49.56%	69.03%
Slovenia		3.13%	97.67%	77.91%	78.29%
Spain		3.73%	97.03%	21.44%	20.00%
Sweden		3.17%	97.63%	19.13%	21.86%



Iceland		1.54%	100.00%	28.57%	71.43%
Liechtenstein		0.00%	0.00%	0.00%	0.00%
Norway		3.30%	95.96%	24.26%	43.01%
Total EU		3.20%	95.84%	28.85%	31.14%
Total EEA		3.20%	95.84%	28.80%	31.30%

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.				
		Number 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		74		26.41%
Belgium		254		37.10%
Bulgaria		91		35.71%
Croatia		13		26.38%
Cyprus		11		34.36%
Czech Republic		399		28.55%
Denmark		414		31.84%
Estonia		11		30.33%
Finland		61		33.60%
France		2,688		37.30%
Germany		2,005		26.78%
Greece		155		30.79%
Hungary		44		32.45%
Ireland		58		29.28%
Italy		314		36.90%
Latvia		4		33.33%
Lithuania		2		29.57%
Luxembourg		6		28.85%
Malta		0		39.10%



Netherlands		127		29.46%
Poland		324		30.81%
Portugal		84		28.31%
Romania		1,126		35.42%
Slovakia		227		28.82%
Slovenia		25		25.24%
Spain		683		34.09%
Sweden		146		31.25%
Iceland		1		22.73%
Liechtenstein		0		11.76%
Norway		61		32.93%
Total EU		9,346		30.95%
Total EEA		9,408		30.95%

Measure 21.2	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 21.2.1	N/A
Measure 21.3	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 21.3.1	N/A



V. Empowering Users

Commitment 22

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

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]	TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 22.1	



QRE 22.1.1	N/A
SLI 22.1.1 - actions enforcing policies above	N/A
	N/A

Measure 22.2	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 22.2.1	N/A
Measure 22.3	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 22.3.1	N/A
Measure 22.4	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 22.4.1	N/A

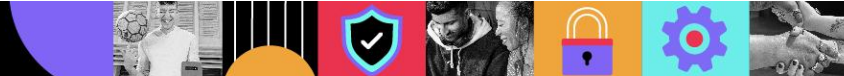


SLI 22.4.1 - actions enforcing policies above	N/A
	N/A
Data	N/A
Measure 22.5	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 22.5.1	N/A
SLI 22.5.1 - actions enforcing policies above	
	N/A

SLI 22.5.2 - actions enforcing policies above	N/A
	N/A
Data	
Measure 22.6	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 22.6.1	N/A
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 (video notice tags, search interventions, public service announcements, in-app information centres 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			



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.

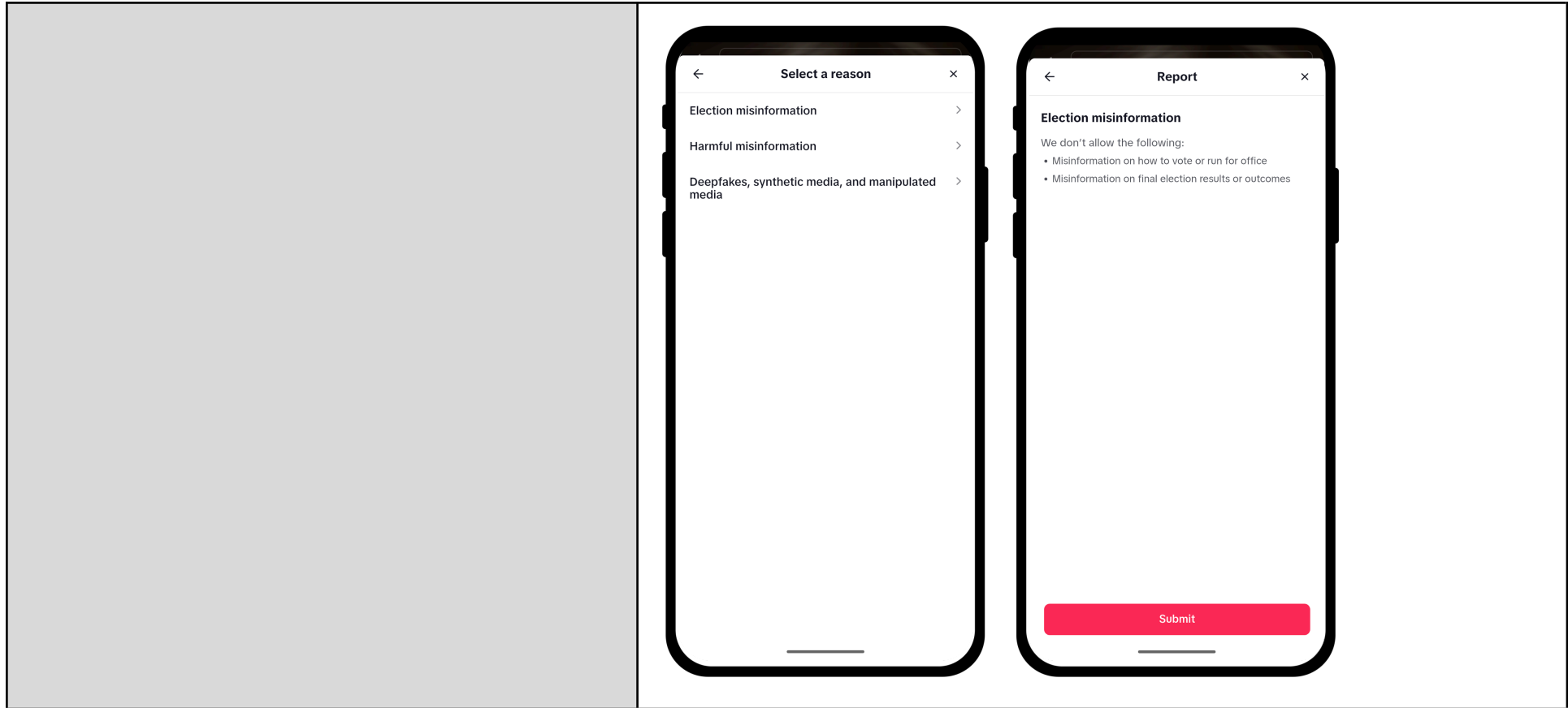
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	<ul style="list-style-type: none"> In line with our DSA requirements, we continued to provide a dedicated reporting channel and appeals process for users who disagree with the outcome, for our community in the European Union to 'Report Illegal Content,' enabling users to alert us to content they believe breaches the law.
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 23.1	
QRE 23.1.1	We provide users with simple, intuitive ways to report/flag content in-app for any breach of our Terms of Service or Community Guidelines including for harmful misinformation in each EU Member State and in an official language of the European Union.

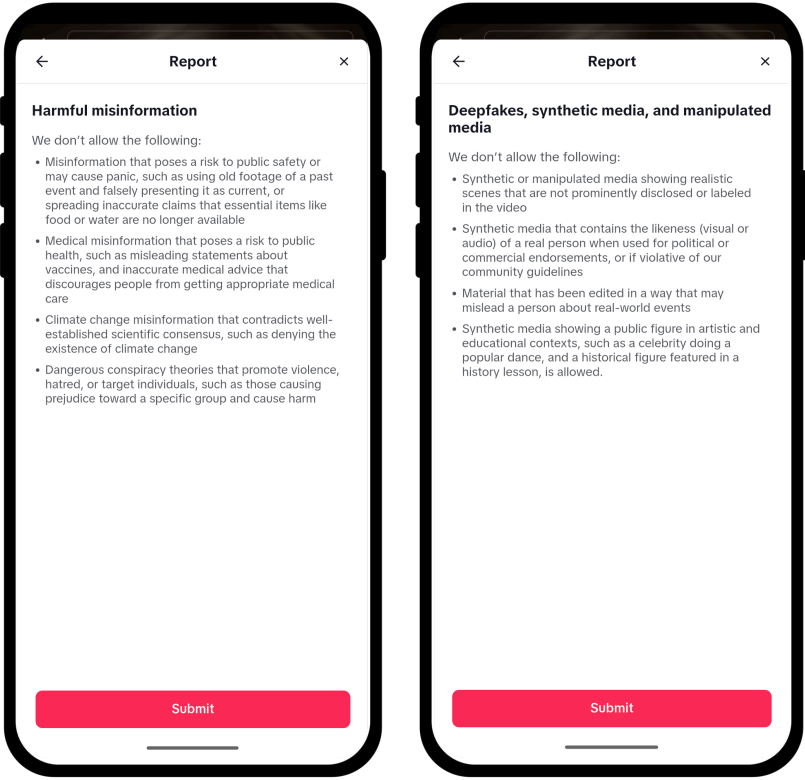


- By 'long-pressing' (e.g., clicking for 3 seconds) on the video content and selecting the "Report" option.
- By selecting the "Share" button available on the right-hand side of the video content and then selecting the "Report" option.

The user is then shown categories of reporting reasons from which to select (which align with the harms our Community Guidelines seek to address). In 2024, we updated this feature to make the "Misinformation" categories more intuitive and allow users to report with increased granularity.

In line with our DSA requirements, we continued to provide a [dedicated reporting channel](#), and appeals process for our community in the European Union to 'Report Illegal Content,' enabling users to alert us to content they believe breaches the law.





People can report TikTok content or accounts without needing to sign in or have an account by accessing the Report function using the “More options (...)” menu on videos or profiles in their browser, or through our “Report Inappropriate content” webform which is available in our [Help Centre](#). Harmful misinformation can be reported across content features such as video, comment, search, hashtag, sound, or account.

Measure 23.2



QRE 23.2.1

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

Reporting system

To ensure the integrity of our reporting system, we deploy a combination of automated review and human moderation.

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 Community Guidelines 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 Community Guidelines, 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 constantly 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.

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.

We have sought to make our Community Guidelines 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).

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 Community Guidelines 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.

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.

Appeals system.

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.

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 Community Guidelines.

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).

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](#).

V. Empowering Users



Commitment 24

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

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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 24.1	
QRE 24.1.1	<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 decision 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	<p>Methodology of data measurement:</p> <p>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, Civic and Election Integrity and Edited media and AIGC policies.</p>			
	Number of actions appealed	Metrics on results of appeals	Number of actions appealed	
List actions per member states and languages (see example table above)	Number of Appeals of videos removed for violation of misinformation policy	Number of overturns of appeals for violation of misinformation policy	Appeal success rate of videos removed for violation of misinformation policy	
Member States				
Austria	609	422	69.3%	



Belgium	809	674	83.3%	
Bulgaria	582	283	48.6%	
Croatia	91	55	60.4%	
Cyprus	92	59	64.1%	
Czech Republic	1,453	468	32.2%	
Denmark	311	226	72.7%	
Estonia	84	49	58.3%	
Finland	207	139	67.1%	
France	6,935	6,296	90.8%	
Germany	12,837	8,939	69.6%	
Greece	705	425	60.3%	
Hungary	228	131	57.5%	
Ireland	948	765	80.7%	
Italy	4,266	3,523	82.6%	
Latvia	110	77	70.0%	
Lithuania	101	84	83.2%	



Luxembourg	35	29	82.9%	
Malta	28	24	85.7%	
Netherlands	1,732	1,441	83.2%	
Poland	5,004	2,065	41.3%	
Portugal	600	393	65.5%	
Romania	5,175	1,539	29.7%	
Slovakia	569	140	24.6%	
Slovenia	96	48	50.0%	
Spain	3,231	2,844	88.0%	
Sweden	658	550	83.6%	
Iceland	13	11	84.6%	
Liechtenstein	2	2	100.0%	
Norway	278	228	82.0%	
Total EU	47,496	31,688	66.7%	
Total EEA	47,789	31,929	66.8%	
List actions per member states and languages (see example table above)	Number of appeals of videos removed for	Number of overruns of appeals for violation	Appeal success rate of videos removed for	



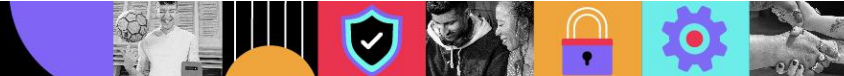
	violation of Civic and Election Integrity policy	of Civic and Election Integrity policy	violation of Civic and Election Integrity policy	
Member States				
Austria	160	124	77.5%	
Belgium	246	196	79.7%	
Bulgaria	58	46	79.3%	
Croatia	14	11	78.6%	
Cyprus	20	15	75.0%	
Czech Republic	162	137	84.6%	
Denmark	102	84	82.4%	
Estonia	15	10	66.7%	
Finland	72	58	80.6%	
France	709	639	90.1%	
Germany	2,844	2,327	81.8%	
Greece	173	139	80.3%	
Hungary	133	102	76.7%	



Ireland	108	97	89.8%	
Italy	1,188	1,048	88.2%	
Latvia	20	13	65.0%	
Lithuania	16	15	93.8%	
Luxembourg	9	7	77.8%	
Malta	0	0	0.0%	
Netherlands	290	236	81.4%	
Poland	423	332	78.5%	
Portugal	154	129	83.8%	
Romania	1,066	855	80.2%	
Slovakia	20	17	85.0%	
Slovenia	7	6	85.7%	
Spain	464	416	89.7%	
Sweden	231	176	76.2%	
Iceland	4	4	100.0%	
Liechtenstein	0	0	0.0%	



Norway	80	68	85.0%	
Total EU	8,704	7,235	83.1%	
Total EEA	8,788	7,307	83.1%	
List actions per member states and languages (see example table above)	Number of appeals of videos removed for violation of Synthetic and Manipulated Media	Number of overtures of appeals for violation of Synthetic and Manipulated Media	Appeal success rate of videos removed for violation of Synthetic and Manipulated Media	
Member States				
Austria	27	24	88.9%	
Belgium	55	48	87.3%	
Bulgaria	21	21	100.0%	
Croatia	7	2	28.6%	
Cyprus	17	11	64.7%	
Czech Republic	72	39	54.2%	
Denmark	40	32	80.0%	
Estonia	8	7	87.5%	
Finland	27	21	77.8%	
France	421	396	94.1%	



Germany	716	542	75.7%	
Greece	55	37	67.3%	
Hungary	6	4	66.7%	
Ireland	36	32	88.9%	
Italy	143	132	92.3%	
Latvia	42	19	45.2%	
Lithuania	22	14	63.6%	
Luxembourg	5	3	60.0%	
Malta	0	0	0.0%	
Netherlands	92	77	83.7%	
Poland	126	87	69.0%	
Portugal	18	14	77.8%	
Romania	158	78	49.4%	
Slovakia	27	19	70.4%	
Slovenia	12	10	83.3%	
Spain	143	130	90.9%	

Sweden	48	40	83.3%	
Iceland	2	2	100.0%	
Liechtenstein	0	0	0.0%	
Norway	32	28	87.5%	
Total EU	2,344	1,839	78.5%	
Total EEA	2,378	1,869	78.6%	



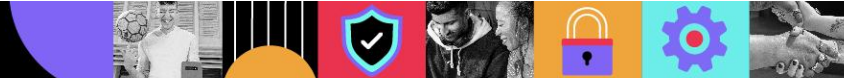
V. Empowering Users

Commitment 25

In order to help users of private messaging services to identify possible disinformation disseminated through such services, Relevant Signatories that provide messaging applications commit to continue to build and implement features or initiatives that empower users to think critically about information they receive and help them to determine whether it is accurate, without any weakening of encryption and with due regard to the protection of privacy.

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]	TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document .
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 25.1	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 25.1.1	N/A
SLI 25.1.1	N/A

	N/A
Data	
Measure 25.2	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 25.2.1	N/A
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].

- Supported new independent research through TikTok's Research Tools (Research API and [VCE](#)).
- Further enriched the data available to include more information on stickers and effects (January) and video tags (April) and reached full parity in data available across the API and VCE (May).
- Added additional functionality to the Research API, including a [compliance API](#) (launched in June) that improves the data refresh process for researchers, helping to ensure that efforts to comply with our Terms of Service (ToS) do not impede researchers' ability to efficiently access data from TikTok's Research API.
- Continued to make the Commercial Content API available in Europe to bring transparency to paid advertising, advertisers and other commercial content on TikTok.
- Continued to offer 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 was active for, the main parameters used for targeting (e.g. age, gender), the number of people who were served the ad.

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]

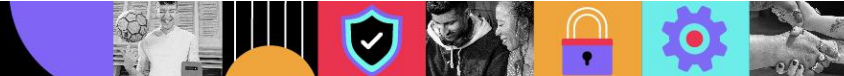
N/A



If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 26.1	
QRE 26.1.1	<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 for EU/EEA countries about our efforts to combat online misinformation. • Our TikTok Community Guidelines Enforcement Reports, providing 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. • We publish monthly Covert Influence Operations Reports, providing more frequent and granular detail about the covert influence operations we have disrupted. • In H1 2025, we launched a new Global Elections Integrity Hub, including dedicated coverage of elections across Europe, the Middle East, and Africa. The Hub outlines our policies, product features, and moderation practices that help protect platform integrity during elections. Throughout this reporting period, we regularly updated the Hub with information on our safety efforts in markets with active elections, including Croatia, Kosovo, Germany, Romania, Portugal, and Poland. <p>As part of our commitment to regulatory transparency and accountability, we launched the European Online Safety Hub, which serves as a 'one-stop-shop' for our community to learn more about how we're complying with the DSA. The Hub is currently available in 22 EU languages and at least one official language of each of the EU Member States. Our dedicated TikTok for Developers website hosts our Research Tools and Commercial Content APIs.(detailed below).</p>



QRE 26.1.2	<p>In this H1 2025 report, TikTok has shared more than 3,000 data points across 30 EU/EEA countries.</p> <p>We provide access to researchers to data that is publicly available on our platform through our Research Tools and through our Commercial Content API for commercial content (detailed below).</p> <p>We also provide ongoing insights into the action we take against content and accounts that violate our Community Guidelines, Terms of Service, or Advertising Policies, in our quarterly TikTok Community Guideline Enforcement Reports. The report includes a variety of data visualisations, which are designed with transparency and accessibility in mind, including for people with colour vision deficiency.</p> <p>As part of our continued efforts to make it easy to study the TikTok platform, the report also offers access to aggregated data, including removal data by policy category, for the 50 markets with the highest volumes of removed content.</p>
SLI 26.1.1	
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 in the US, EEA, UK and Switzerland, with access to public data on accounts and content, including comments, captions, subtitles, number of comments, shares, likes, followers and following lists, and favourites that a video receives on our platform. More information is available here. We carefully consider feedback from researchers who have used the API and continue to make improvements such as additional data fields, streamlining the application process, and enabling collaboration through Lab Access, which allows up to 10 researchers to work together on a shared research project.</p>



	<p>(II) Virtual Compute Environment (VCE)</p> <p>The VCE allows qualifying not-for-profit researchers in the EU to access and analyse TikTok's public data, while ensuring robust security and privacy protections. Public data can be accessed and analysed in 2 stages:</p> <ol style="list-style-type: none"> 1. Test Stage: Query the data using TikTok's query software development kit (SDK). The VCE will return random sample data based on your query, limited to 5,000 records per day. 2. Execution Stage: Submit a script to execute against all public data. TikTok provides a powerful search capability that allows data to be paginated in increments of up to 100,000 records. TikTok will review the results file to make sure the output is aggregated. <p>(III) 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 API that includes ads, ad and advertiser metadata, and targeting information. Researchers and professionals are required to create a TikTok for 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>(IV) 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>(I) Research API</p> <p>Through our Research API, academic researchers from non-profit academic institutions in the US and Europe, can apply to study public data about TikTok content and accounts. This public</p>



	<p>data includes comments, captions, subtitles, number of comments, shares, likes, followers and following lists, and favourites that a video receives on our platform. More information is available here.</p> <p>(II) Virtual Compute Environment (VCE)</p> <p>Through our VCE, qualifying not-for-profit researchers and academic researchers from non-profit academic institutions in the EU can query and analyse TikTok's public data. To protect the security and privacy of our users the VCE is designed to ensure that TikTok data is processed within confined parameters. TikTok only reviews the results to ensure that there is no identifiable individual information extracted out of the platform. All aggregated results will be shared as a downloadable link to the approved primary researcher's email.</p> <p>(III) Commercial Content API</p> <p>Through our Commercial Content API, qualifying researchers and professionals, who can be located in any country, can request public data about commercial content including ads, ad and advertiser metadata, and targeting information. To date, the Commercial Content API only includes data from EU countries.</p> <p>(IV) Commercial Content Library</p> <p>TikTok's Commercial Content Library is a repository of ads and other types of commercial content posted to users in the European Economic Area (EEA), Switzerland, and the UK only, but can be accessed by members of the public located in any country. Each ad and ad details will be available in the library for one year after the advertisement was last viewed by any user. Through the 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 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 is not a paid ad.</p>
QRE 26.2.3	<p>We make detailed information available to applicants about our Research Tools (Research API and VCE) and Commercial Content API, through our dedicated TikTok for Developers website, including on what data is made available and how to apply for access.</p>



	<p>Once an application has been approved for access to our Research Tools, 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>					
SLI 26.2.1	<p>Research Tools, Commercial Content API, and the Commercial Content Library</p> <p>During this reporting period we received:</p> <ul style="list-style-type: none"> 173 applications to access TikTok's Research Tools (Research API and VCE) from researchers in the EU and EEA. 74 applications to access the TikTok Commercial Content API. 					
	Number of applications received for Research Tools	Number of applications accepted for Research Tools	Number of applications rejected for Research Tools	Number of applications received for TikTok Commercial Content API	Number of applications accepted for TikTok Commercial Content API	Number of applications rejected for TikTok Commercial Content API
Austria	6	6	4	1	1	0
Belgium	2	1	0	1	1	0
Bulgaria	0	0	0	0	0	0
Croatia	0	0	1	0	0	0
Cyprus	0	0	0	0	0	0
Czech Republic	5	3	1	2	2	0
Denmark	5	5	2	1	1	0
Estonia	0	0	0	0	0	0
Finland	2	1	0	0	0	0



France	16	11	11	24	19	3
Germany	48	50	21	11	10	1
Greece	1	2	0	2	2	0
Hungary	0	0	0	2	1	0
Ireland	3	1	3	1	0	1
Italy	21	16	6	1	1	0
Latvia	0	0	0	3	3	0
Lithuania	0	0	0	0	0	0
Luxembourg	0	0	0	0	0	0
Malta	0	0	0	0	0	0
Netherlands	13	9	12	3	2	0
Poland	4	3	1	4	4	0
Portugal	0	0	0	3	3	0
Romania	4	3	3	2	2	0
Slovakia	1	0	0	2	1	1
Slovenia	2	1	1	1	1	0
Spain	32	12	18	7	5	2
Sweden	6	5	2	3	3	0
Iceland	0	0	0	0	0	0



Lichtenstein	0	0	0	0	0	0
Norway	2	2	1	0	0	0
EU Level	171	129	86	74	62	8
EEA Level	173	131	87	74	62	8
Measure 26.3						
QRE 26.3.1	We welcome feedback from researchers on our APIs and have a dedicated support form where researchers can provide feedback about their experience. On foot of recent feedback, we launched the new batch compliance APIs allowing researchers to comply with the refresh requirements defined in our Terms of Service without using their daily quota limit.					

VI. Empowering the research community	
Commitment 27	
Relevant Signatories commit to provide vetted researchers with access to data necessary to undertake research on Disinformation by developing, funding, and cooperating with an independent, third-party body that can vet researchers and research proposals.	
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]	TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document .
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	N/A



the 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 27.1	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 27.1.1	N/A
Measure 27.2	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 27.2.1	N/A
Measure 27.3	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 27.3.1	N/A
SLI 27.3.1 - research projects vetted by the independent third-party body	N/A
	N/A
Data	N/A
Measure 27.4	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .



QRE 27.4.1	N/A
------------	-----

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
If yes, list these implementation measures here [short bullet points].	<ul style="list-style-type: none"> Supported new independent research through TikTok's Research Tools (Research API and VCE). Enriched the data available to include more information on stickers and effects (January) and video tags (April) and reached full parity in data available across the API and VCE (May). Added additional functionality to the Research API, including a compliance API (launched in June) that improves the data refresh process for researchers, helping to ensure that efforts to comply with our Terms of Service (ToS) does not impede researchers' ability to efficiently access data from TikTok's Research API. Continued to make the Commercial Content API available in Europe to bring transparency to paid advertising, advertisers and other commercial content on TikTok. Continued to offer 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 was active for, the main parameters used for targeting (e.g. age, gender), the number of people who were served the ad.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve	N/A



the 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 28.1	
QRE 28.1.1	<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 Tools, Commercial Content APIs and Commercial Content Library, full details of which are available on our TikTok for Developers and Commercial Content Library websites.</p> <p>We have many teams and individuals across product, policy, data science, outreach and legal working to facilitate research. We believe transparency and accountability are essential to fostering trust with our community. We are committed to transparency in how we operate, moderate and recommend content, empower users, and secure our platform. That's why we opened our global Transparency and Accountability Centers (TACs) for invited guests to see first-hand our work to protect the safety and security of the TikTok platform.</p> <p>Our TACs are located in Dublin, Los Angeles, Singapore, and Washington, DC. They provide an opportunity for invited academics, businesses, policymakers, politicians, regulators, researchers and many other expert audiences from Europe and around the world to see first-hand how teams at TikTok go about the critically important work of securing our community's safety, data, and privacy. During the reporting period, DubTAC hosted 24 external tours, welcoming over 180 visitors. Notable attendees included: Ofcom; the EU Commission and representatives from the Irish Parliament; French; Danish; German; and UAE governments. We also welcomed mental health organisations and brand clients, including Coca Cola and Zalando. In March, we launched Mobile TAC in Brussels during Global Marketing Week and delivered 5 Mobile TAC tours across the EU.</p>



We work closely with our ten regional [Advisory Councils](#), including our European Safety Advisory Council and US Content Advisory Council, and our global [Youth Advisory Council](#), which bring together a diverse array of independent experts from academia and civil society as well as youth perspectives. 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, including in the development of our [AI-generated content label](#) and a recent campaign to raise awareness around AI labeling and potentially misleading AIGC. These councils are an important way to bring outside perspectives into our company and onto our platform.

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.

Our **Outreach and Partnerships Management (OPM) 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 global experts, including numerous academics in Europe, in the development of our state-affiliated media policy, Election Misinformation policies, and AI-generated content labels. OPM also plays an important role in our efforts to counter misinformation by identifying, onboarding and managing new partners to our fact-checking programme. In the lead-up to certain elections, we invite suitably qualified external local/regional experts, as part of our Election Speaker Series. Sharing their market expertise with our internal teams provides us with insights to better understand areas that could potentially amount to election manipulation, and informs our approach to the upcoming election.

During this reporting period, we ran 7 Election Speaker Series sessions, 3 in EU Member States and 4 in Albania, Belarus, Greenland, and Kosovo.

1. Albania: Internews Kosova (Kallxo)
2. Belarus: Belarusian Investigative Center
3. Germany: Deutsche Presse-Agentur (dpa)
4. Greenland: Logically Facts
5. Kosovo: Internews Kosova (Kallxo)
6. Poland: Demagog



	<p>7. Portugal: Poligrafo</p> <p>TikTok teams and personnel also regularly participate in research-focused events. In H1 2025, we presented at the Political Tech Summit in Berlin (January), hosted Research Tools demos in Warsaw (April), presented at GNET Annual Conference (May), hosted Research Tools demos in Prague (June), presented at the Warsaw Women in Tech Summit (June), briefed a small group of Irish academic researchers (June), and attended the ICWSM conference in Copenhagen (June).</p> <p>At the end of June 2025, we sent a 14 strong delegation to GlobalFact12 in Rio de Janeiro, Brazil. TikTok was a top-tier sponsor of GlobalFact. Sponsorship money supports IFCN's work serving the fact-checking community and makes the conference itself possible for fact-checking organizations to attend through providing travel scholarships. The annual conference represents the most important industry event for TikTok's Global Fact-Checking Program and covers a broad set of topics related to mis- and dis-information that are discussed in main stage sessions and break-out rooms. In addition to a breakout session on Footnotes, TikTok hosted a networking event with more than 80 people from our partner organizations, including staff from fact checking partners, media literacy organizations, and TikTok's Safety Advisory Councils.</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 our Research Tools and Commercial Content APIs.</p> <p>With the Research API, researchers can access:</p> <ul style="list-style-type: none"> • Public account data, such as user profiles, followers and following lists, liked videos, pinned videos and reposted videos. • Public content data, such as comments, captions, subtitles, and number of comments, shares and likes that a video receives.



	<p>Through the VCE, qualifying not-for-profit researchers in the EU can access and analyse TikTok's public data, including public U18 data, in a secure environment that is subject to strict security controls.</p> <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 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	<p>The data we make available and the application criteria for our Research Tools (Research API and VCE) and Commercial Content API is research topic agnostic and clearly set out in our dedicated TikTok for Developers website. In August 2024, introduced a due diligence process with an external vendor to confirm the eligibility of NGO applicants.</p>
Measure 28.4	<p>TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document.</p>
QRE 28.4.1	N/A



VI. Empowering the research community

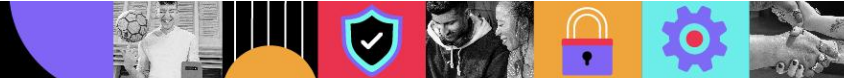
Commitment 29

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]	TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document .
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 29.1	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 29.1.1	N/A
QRE 29.1.2	N/A
QRE 29.1.3	N/A



SLI 29.1.1 - reach of stakeholders or citizens informed about the outcome of research projects	N/A
	N/A
Data	N/A
Measure 29.2	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 29.2.1	N/A
QRE 29.2.2	N/A
QRE 29.2.3	N/A
SLI 29.2.1	N/A
	N/A
Data	N/A
Measure 29.3	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 29.3.1	N/A
SLI 29.3.1 - reach of stakeholders or citizens informed about the outcome of research projects	N/A
	N/A
Data	N/A



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

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"> Updated fact checking agreements to include the requirement that factfact checking partners provide regular pro-active Insights Reports about general misinformation trends observed on our platform and across the industry generally, including new/changing industry or market trends, events or topics that generate particular misinformation or disinformation.
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 30.1	



QRE 30.1.1	<p>Within Europe, we work with 12 fact-checking partners who provide fact-checking coverage in 23 EEA languages, including at least one official language of every EU Member State, and additional languages including Georgian, Russian, Turkish, Ukrainian, Albanian and Serbian.</p> <p>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 of common standards and conditions. We reviewed and updated 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, and will provide regular pro-active Insights Reports about general misinformation trends observed on our platform and across the industry generally, including new/changing industry or market trends, events or topics that generate particular misinformation or disinformation. • 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 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.
QRE 30.1.2	<p>We currently have 12 IFCN accredited fact-checking partners across the EU, EEA, and wider Europe:</p> <ol style="list-style-type: none"> 1. Agence France-Presse (AFP) 2. Deutsche Presse-Agentur (dpa) 3. Demagog 4. Facta



5. Geofacts
6. Faktograf
7. Internews Kosova (Kallxo)
8. Lead Stories
9. Newtral
10. Poligrafo
11. Reuters
12. Teyit

These partners provide fact-checking coverage in 23 official EEA languages, including at least one official language of each EU Member States, and additional languages including Georgian, Russian, Turkish, Ukrainian, Albanian and Serbian.

We can, and have, put in place temporary agreements with these fact-checking partners to provide additional EU language coverage during high risk events like elections or an unfolding crisis.

Outside of our fact-checking program, we also collaborate with fact-checking organisations to develop a variety of media literacy campaigns. For example, during this reporting period, we worked with European fact-checkers on 9 temporary **media literacy campaigns**, in advance of regional elections, through our in-app Election Centers:

- 7 in the EU
 - Croatia (local election): Faktograf
 - Croatia (presidential election): Faktograf
 - Germany: Deutsche Presse-Agentur (dpa)
 - Latvia: Lead Stories
 - Poland: Demagog and FakeNews.pl
 - Portugal: Poligrafo
 - Romania: Funky Citizens
- 2 in wider European/regionally relevant countries
 - Albania: Internews Kosova (Kallxo)
 - Greenland: Logically Facts

We also rolled out three new ongoing **general media literacy and critical thinking skills campaigns** in the EU in collaboration with our fact-checking and media literacy partners:



	<ul style="list-style-type: none"> ○ Germany: Deutsche Presse-Agentur (dpa) ○ Romania: Funky Citizens, Digi Media, and Libertatea ○ Poland: Demagog, FakeNews.pl, Radio Zet, and Orientuj.sie <p>Globally, we have 21 IFCN-accredited fact-checking partners. We are continuously working to expand our fact-checking network and we keep users updated here.</p>
<p>QRE 30.1.3</p>	<p>We have fact-checking coverage in 23 official EEA languages: Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish.</p> <p>We have fact-checking coverage in a number of other European languages or languages which affect European users, including Georgian, Russian, Turkish, and Ukrainian and we can request additional support in Azeri, Armenian, and Belarusian.</p> <p>In terms of global fact-checking initiatives, we currently cover more than 60 languages and 130 markets across the world, thereby improving the overall integrity of the service and benefiting European users.</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. ● Insights reports. Our fact-checking partners provide 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. Where relevant, we create guidelines and trending topic reminders for our moderators which are informed by previous fact checking



assessments. This helps our moderation teams leverage the insights from our fact-checking partners and supports swift and accurate decisions on flagged content regardless of the language in which the original claim was made.

- **Election Speaker Series.** To further promote election integrity, and inform our approach to country-level EU and regionally relevant 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 the following organisations:
 - Albania: Internews Kosova (Kallxo)
 - Belarus: Belarusian Investigative Center
 - Germany: Deutsche Presse-Agentur (dpa)
 - Greenland: Logically Facts
 - Kosovo: Internews Kosova (Kallxo)
 - Poland: Demagog
 - Portugal: Poligrafo

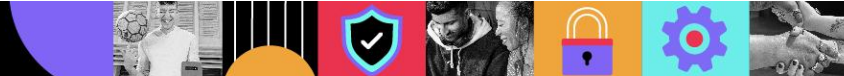
Moderation teams working dedicated misinformation queues receive enhanced training on our misinformation policies and have access to the above-mentioned tools and measures, which enables them to make accurate content decisions across Europe and globally.

We place considerable emphasis on proactive detection to remove violative content and reduce exposure to potentially distressing content for our human moderators. Before content is posted to our platform, it's reviewed by automated moderation technologies which identify content or behavior that may violate our policies or For You feed eligibility standards, or that may require age-restriction or other actions. While undergoing this review, the content is visible only to the uploader.

If our automated moderation technology identifies content that is a potential violation, it will either take action against the content or flag it 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.

Some of the methods and technologies that support these efforts include:

- **Vision-based:** Computer vision models can identify objects that violate our Community Guidelines—like weapons or hate symbols.



	<ul style="list-style-type: none"> • Audio-based: Audio clips are reviewed for violations of our Community Guidelines, supported by a dedicated audio bank and "classifiers" that help us detect audios that are similar or modified to previous violations. • Text-based: Detection models review written content like comments or hashtags, using foundational keyword lists to find variations of violative text. "Natural language processing"—a type of Artificial Intelligence (AI) that can interpret the context surrounding content—helps us identify violations that are context-dependent, such as words that can be used in a hateful way but may not violate our policies by themselves. We also work with various external experts, like our fact-checking partners, to inform our keyword lists. • Similarity-based: "Similarity detection systems" enable us to not only catch identical or highly similar versions of violative content, but other types of content that share key contextual similarities and may require additional review. • Activity-based: Technologies that look at how accounts are being operated help us disrupt deceptive activities like bot accounts, spam, or attempts to artificially inflate engagement through fake likes or follow attempts. • LLM-based: We're starting to use a kind of AI called "large language learning models" to scale and improve content moderation. LLMs can comprehend human language and perform highly specific, complex tasks. This can make it possible to moderate content with a higher degree of precision, consistency and speed than human moderation. • Multi-modal LLM-based: "Multi-modal LLMs" can also perform complex, highly specific tasks related to other types of content, such as visual content. For example, we can use this technology to make misinformation moderation easier by extracting specific misinformation "claims" from videos for moderators to assess directly or route to our fact-checking partners. • Content Credentials: We launched the ability to read Content Credentials that attach metadata to content, which we can use to automatically label AI-generated content that originated on other major platforms. <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	Fact-checking coverage implemented
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	Fact-checking coverage implemented
Lithuania	Fact-checking coverage implemented



Luxembourg	Fact-checking coverage implemented
Malta	No permanent fact-checking coverage. We can, and have, put in place temporary agreements with fact-checking partners to provide additional EU language coverage during high risk events like elections or an unfolding crisis. 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	Fact-checking coverage implemented
Spain	Fact-checking coverage implemented
Sweden	Fact-checking coverage implemented
Iceland	No permanent fact-checking coverage. We can, and have, put in place temporary agreements with fact-checking partners to provide additional EU language coverage during high risk events like elections or an unfolding crisis. 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 languages



Total EEA	23 languages
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, 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 them and provide data regarding their feedback and also conduct surveys with them.</p>
QRE 30.2.2	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.
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 through individual feedback sessions, and active participation in global fact-checking events, such as GlobalFact12 (June 2025), where we hosted a networking event with more than 80 people from our partner organizations, including staff from fact checking partners, media literacy organizations, and TikTok's Safety Advisory Councils.</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	
Relevant Signatories commit to integrate, showcase, or otherwise consistently use fact-checkers' work in their platforms' services, processes, and contents; with full coverage of all Member States and languages.	
In 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 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). Conducted feedback sessions with our partners to further enhance the efficiency of the fact-checking program.



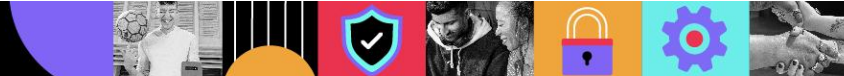
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 31.1	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
Measure 31.2	
QRE 31.1.1	<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 work with 12 fact-checking partners in Europe, covering 23 EEA languages.</p> <p>As previously outlined, we place considerable emphasis on proactive detection and automated moderation technology to action violative content. For example, "multi-modal LLMs" can perform complex, highly specific tasks related to visual content. We can use this technology to make misinformation moderation easier by extracting specific misinformation "claims" from videos for moderators to assess directly or route to our fact-checking partners.</p> <p>Our content moderation team receives specialised training to 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:</p> <p>(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.</p> <p>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.</p>



	<p>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 Community Guidelines and what action to take.</p> <p>(ii) contributing to our global database of previously fact-checked claims to help our misinformation moderators make decisions.</p> <p>(iii) a proactive detection programme with our fact-checkers who flag new and evolving claims they're seeing on our platform. This enables our moderators to quickly assess these claims and remove violations.</p> <p>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 anyone's For You feed to limit the spread of potentially misleading information.</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 reviewed by one of our fact-checking partners in the relevant territory.</p>			
	Number 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	111			



Belgium	278			
Bulgaria	1,514			
Croatia	189			
Cyprus	14			
Czech Republic	210			
Denmark	293			
Estonia	298			
Finland	177			
France	2,705			
Germany	2,028			
Greece	116			
Hungary	220			
Ireland	61			
Italy	312			
Latvia	131			
Lithuania	166			
Luxembourg	14			
Malta	3			
Netherlands	132			



Poland	920			
Portugal	290			
Romania	1,821			
Slovakia	194			
Slovenia	153			
Spain	215			
Sweden	272			
Iceland	2			
Liechtenstein	0			
Norway	183			
Total EU	12,837			
Total EEA	13,022			

SLI 31.1.2 - impact of actions taken	Methodology of data measurement: 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. These metrics correspond to the numbers of removals under the misinformation policy since all of its enforcement are based on the policy guidelines, known misinformation trends and knowledge-based repository.			
	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	25	2,709	
Belgium	17	3,853	
Bulgaria	323	3,368	
Croatia	64	495	
Cyprus	4	441	
Czech Republic	46	4,134	
Denmark	15	1,267	
Estonia	45	305	
Finland	22	2,451	
France	124	37,041	
Germany	383	47,342	
Greece	16	3,094	
Hungary	19	1,110	
Ireland	3	2,850	
Italy	69	19,673	



Latvia	10	412	
Lithuania	15	494	
Luxembourg	0	545	
Malta	0	504	
Netherlands	9	6,426	
Poland	197	16,929	
Portugal	30	2,791	
Romania	378	24,291	
Slovakia	51	3,301	
Slovenia	30	2,710	
Spain	30	16,368	
Sweden	23	2,742	
Iceland	0	73	
Liechtenstein	0	6	
Norway	12	1,378	
Total EU	1,948	207,646	
Total EEA	1,960	209,103	

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 harmful misinformation policy.
List actions per member states and languages (see example table above)	Videos removed as a result of a fact checking assessment as a percentage of total number of videos removed due to violation of harmful misinformation policy
Austria	0.9%
Belgium	0.4%
Bulgaria	9.6%
Croatia	12.9%
Cyprus	0.9%
Czech Republic	1.1%
Denmark	1.2%
Estonia	14.8%
Finland	0.9%
France	0.3%
Germany	0.8%



Greece	0.5%
Hungary	1.7%
Ireland	0.1%
Italy	0.4%
Latvia	2.4%
Lithuania	3.0%
Luxembourg	0.0%
Malta	0.0%
Netherlands	0.1%
Poland	1.2%
Portugal	1.1%
Romania	1.6%
Slovakia	1.5%
Slovenia	1.1%
Spain	0.2%
Sweden	0.8%
Iceland	0.0%
Liechtenstein	0.0%
Norway	0.9%



Total EU	0.938%
Total EEA	0.937%

Measure 31.3	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 31.3.1	N/A
Measure 31.4	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document .
QRE 31.4.1	N/A

VII. Empowering the fact-checking community	
<p>Commitment 32</p> <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>	
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

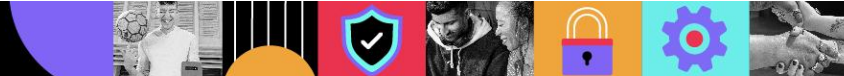


If yes, list these implementation measures here [short bullet points].	Continued to explore ways to improve data sharing in connection with our pilot scheme to share enforcement data with our fact-checking partners on the claims they have provided feedback on.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 32.1	
Measure 32.2	
QRE 32.1.1	<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>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>
SLI 32.1.1 - use of the interfaces and other tools	<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>



Data			
Measure 32.3			
QRE 32.3.1	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.		

VII. Empowering the fact-checking community	
<p style="text-align: center;">Commitment 33</p> <p style="text-align: center;">Relevant Signatories (i.e. fact-checking organisations) commit to operate on the basis of strict ethical and transparency rules, and to protect their independence.</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]	TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document .
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]	N/A



If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 33.1	TikTok did not subscribe to this measure as outlined in the January 2025 Subscription Document
QRE 33.1.1	N/A
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].	We have been an active participant in the working group that has successfully launched the common Transparency Centre in 2023. We held the position of co-chair of the Transparency working group since September 2023, before the position was transferred to VOST, a civil society organisation that is a signatory of the Code. From January 2024, we supported the transition of the maintenance and development of the website from the former third-party vendor, to the signatory of the Code, Vost.eu . We supported VOST as it launched the new Transparency Center after the publication of the previous report covering H2 2024.
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
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]	No, through our participation in the Transparency Centre working group, we have ensured that the Transparency 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 by signatory).
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A



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

VIII. Transparency Centre	
<p>Commitment 36</p> <p>Signatories commit to updating the relevant information contained in the Transparency Centre in a timely and complete manner.</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
Do you plan to put further implementation measures in place in the next 6 months to substantially improve	N/A



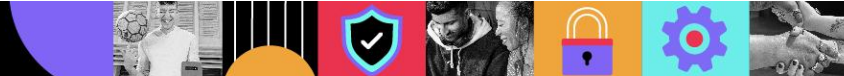
the maturity of the implementation of this commitment? [Yes/No]	
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 36.1	
Measure 36.2	
Measure 36.3	
QRE 36.1.1 (for the Commitments 34-36)	The Transparency Centre was successfully launched in February 2023. We continue to upload our report according to the approved deadlines.
QRE 36.1.2 (for the Commitments 34-36)	The administration of the Transparency Centre website has been transferred fully to the community of the Code's signatories, with VOST Europe taking the role of developer.
SLI 36.1.1	We worked with the vendor to develop relevant metrics for this SLI.
Data	Between January 1 and June 30 2025, our signatory profile was visited 729 times, and our signatory reports were downloaded 6,858 times. The Transparency Centre Webpage overall was visited 35,760 times.



IX. Permanent Task-Force Commitment 37



IX. Permanent Task-Force	
<p style="text-align: center;">Commitment 37</p> <p>Signatories commit to participate in the permanent Task-force. The Task-force includes the Signatories of the Code and representatives from EDMO and ERGA. It is chaired by the European Commission, and includes representatives of the European External Action Service (EEAS). The Task-force can also invite relevant experts as observers to support its work. Decisions of the Task-force are made by consensus.</p>	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No
If yes, list these implementation measures here [short bullet points].	We have meaningfully engaged in the Task-force / Plenaries and all working groups.
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 37.1	
Measure 37.2	
Measure 37.3	



Measure 37.4	
Measure 37.5	
Measure 37.6	
QRE 37.6.1	<p>We have meaningfully engaged in the Task-force and all of its working groups by attending and participating in meetings and engaging in any relevant discussions, in particular regarding elections and further developing/activating the Rapid Response System (RRS).</p> <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 - 43



X. Monitoring of Code	
<p>Commitment 38</p> <p>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.</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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 38.1	



QRE 38.1.1	<p>TikTok 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.</p> <p>Across the European Union, we have thousands of trust and safety professionals dedicated to keeping our platform safe. We also 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	
<p style="text-align: center;">Commitment 39</p> <p style="text-align: center;">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>	
<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>TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document.</p>
<p>If yes, list these implementation measures here [short bullet points].</p>	<p>N/A</p>
<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>N/A</p>



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

X. Monitoring of Code	
<p style="text-align: center;">Commitment 40</p> <p>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.</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].	We have reported on the SLIs and QREs relevant to the Commitments we signed-up to within 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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 40.1	



Measure 40.2	
Measure 40.3	
Measure 40.4	
Measure 40.5	
Measure 40.6	

X. Monitoring of Code	
<p style="text-align: center;">Commitment 41</p> <p>Signatories commit to work within the Task-force towards developing Structural Indicators, and publish a first set of them within 9 months from the signature of this Code; and to publish an initial measurement alongside their first full report. To achieve this goal, Signatories commit to support their implementation, including the testing and adapting of the initial set of Structural Indicators agreed in this Code. This, in order to assess the effectiveness of the Code in reducing the spread of online disinformation for each of the relevant Signatories, and for the entire online ecosystem in the EU and at Member State level. Signatories will collaborate with relevant actors in that regard, including ERGA and EDMO.</p>	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No, pending further updates from the Commission.
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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 41.1	
Measure 41.2	
Measure 41.3	

X. Monitoring of Code	
<p style="text-align: center;">Commitment 42</p> <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].	We have been an active participant in the Crisis Response working group, which resulted in the implementation of the Rapid Response System being developed/ activated for elections. We have also published Crisis Reports specific to the War in Ukraine, the Israel/Hamas conflict and



	2025 elections reports on the Polish Presidential, Romanian Presidential Election, German Federal Election, and Portuguese Legislative Election 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]	N/A
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A

X. Monitoring of Code	
<p>Commitment 43</p> <p>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.</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"> • Participated in the monitoring and reporting working group. • Published transparency report in March 2025.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve	N/A

the 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



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**”) continues to challenge us to confront an incredibly complex and continually evolving 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 in Ukraine in the reporting period. We remain committed to preventing such content from being shared in this context.

(I) Spread of harmful misinformation

We observe and take action where appropriate under our policies. Since the War in Ukraine began 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.

TikTok adopts a dynamic approach to understanding and removing misleading stories. When addressing harmful misinformation, we apply our [Integrity and Authenticity policies](#) (**Integrity and Authenticity policies**) in our [Community Guidelines](#) and we will take action against offending content on our platform. Our moderation teams are provided with detailed policy guidance and direction when moderating on crisis related misinformation using our misinformation policies, this includes the provision of case banks of harmful misinformation claims to support their moderation work.

(II) CIOs

We continuously work to detect and disrupt covert influence operations that attempt to establish themselves on TikTok and undermine the integrity of our platform. Our Integrity and Authenticity 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 that are on high alert to investigate and detect CIOs on our platform. We ban accounts that try to engage in such behavior, take action on others that we assess as part of the network, and report them regularly in our Transparency Center. When we ban these accounts, any content they posted is also removed.

In the period from January to June 2025, we took action to remove a total of 7 networks (consisting of 29,245 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 new dedicated CIO transparency report [here](#).



CIO will continue to evolve in response to our detection, and networks may attempt to reestablish a presence on our platform. To counter these emerging threats and stay ahead of evolving challenges, we have expert teams who focus entirely on detecting, investigating, and disrupting covert influence operations.

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

We aim 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 such as the War in Ukraine.

(I) Investment in our fact-checking programme

We employ a layered approach to detecting harmful misinformation that is in violation of our Community Guidelines.

Working closely with our fact-checking partners is a crucial part of our approach to enforcing harmful misinformation on our platform. Our fact-checking programme includes coverage of Russian, Ukrainian, and Belarusian. We also partner with Reuters, which is dedicated to helping us accurately fact-check content in Russian and Ukrainian.

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

(II) Disruption of CIOs

As set out above, disrupting CIO networks has been high priority for us in the context of the crisis. We published a list of the networks we disrupted in the relevant period within our most recently published transparency report [here](#).

Between January and June 2025, we took action to remove a total of 7 networks (consisting of 29,245 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 dedicated CIO transparency report [here](#).

Countering influence operations is an industry-wide effort, in part because these operations often spread their activity across multiple platforms. We regularly consult with third-party experts, including our global [Content and Safety Advisory Councils](#), whose guidance helps us improve our policies and understand regional context.

(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. Our state-affiliated media policy is used to help users understand the context of certain content and to help them to evaluate the content they consume on our platform. Labels have since applied to content posted by the state-affiliated accounts of such entities in Russia, Ukraine and Belarus.



We continue the detection and labeling of state-controlled media accounts in accordance with our state-controlled media label policy globally.

(IV) Mitigating the risk of monetisation of harmful misinformation

Political advertising has been prohibited on our platform for many years, but as an additional risk mitigation measure against the risk of profiteering from the War in Ukraine we prohibit Russian-based advertisers from outbound targeting of EU markets. We also suspended TikTok in the Donetsk and Luhansk regions, removing Livestream videos originating in Ukraine from the For You feed of users located in the EU. In addition, the ability to add new video content or Livestream videos to the platform in Russia remains suspended.

(V) Launching localised media literacy campaigns

Proactive measures aimed at improving our users' digital literacy are vital, and we recognise the importance of increasing the prominence of authoritative information. We have thirteen localised media literacy campaigns addressing disinformation related to the War in Ukraine in Austria, Bulgaria, Czech Republic, Croatia, Estonia, Germany, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia, and Slovenia in close collaboration with our factchecking 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. We have also partnered with a local Ukrainian fact-checking organisation, VoxCheck, with the aim of launching a permanent media literacy campaign in Ukraine.

[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].

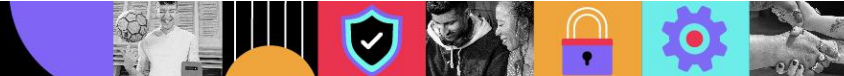
Policies and Terms and Conditions

Outline any changes to your policies

Policy	Changes (such as newly introduced policies, edits, adaptation in scope or implementation)	Rationale
No relevant updates in the reporting period.	N/A In a crisis, we keep under review our policies and to ensure	Our Integrity and Authenticity policies are our first line of defense in combating harmful misinformation and deceptive behaviours on our platform. Our Community Guidelines make clear to our users what content we remove or make ineligible for the For You feed when it poses a risk of harm to our users or the wider public. Our moderation teams are



	<p>moderation teams have supplementary guidance.</p> <p>provided with detailed policy guidance and direction when moderating on war-related harmful misinformation using existing policies.</p> <p>We have specialist teams within our Trust and Safety department dedicated to the policy issue of Integrity and Authenticity, including within the areas of product and policy. Our experienced subject matter experts on Integrity and Authenticity 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, our teams work to ensure that appropriate guidance is developed so that the Integrity and Authenticity policies are applied effectively in respect of content relating to the relevant crisis (in this case, the war). This includes issuing detailed policy guidance and direction, including providing case banks on harmful misinformation claims to support moderation teams.</p>
Scrutiny of Ads Placements	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
<p>Preventing misuse of our monetisation features (Commitment 1, Measure 1.1)</p>	<p>Description of intervention</p> <p>TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document</p>
	<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 to identify content that breaches our ad policies.</p> <p>We enforce our strict ad policies and have expert teams focused on investigating and responding to any attempts to circumvent them.</p>



	<p><i>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</i></p> <p>Our efforts on ad moderation practices help to ensure that ads that breach our policies are rejected or removed, both in the context of the War in Ukraine and more broadly on our platform.</p>
Political Advertising	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
<p>Prohibition on Political Advertising (Commitment 4)</p>	<p><i>Description of intervention</i></p> <p>TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document</p>
	<p><i>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</i></p> <p>N/A</p>
Integrity of Services	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
<p>Identifying and removing CIO networks (Commitment 14, Measure 14.1)</p>	<p><i>Description of intervention</i></p> <p>We fight against CIO as our Integrity and Authenticity 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 prohibit and constantly work to disrupt attempts to engage in covert influence operations by manipulating our platform and/or harmfully misleading our community, our expert teams that focus entirely on detecting, investigating, and disrupting CIO networks that have removed numerous networks targeting discourse about the War in Ukraine.</p>



	<p>Countering covert influence operations is a particular challenge because the adversarial actors behind them continuously evolve the ways they hide the linkage between their accounts. Our experts work to counter covert influence operations by studying the many layers of techniques, tactics, and procedures that deceptive actors use to try to manipulate platforms, drawing from a variety of disciplines, including threat intelligence and data science.</p>
	<p><i>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</i></p> <p>Between January and June 2025, we took action to remove the following 7 networks (consisting of 29,245 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>Network Origin: Moldova Description: We assess that this network operated from Moldova and targeted a Russian-speaking audience in Moldova and Ukraine. The individuals behind this network created inauthentic accounts in order to discredit the government of Moldova within the context of the 2024 Moldovan presidential elections. The network was also found, to a lesser extent, to post content undermining the mobilization processes in Ukraine. Accounts Removed: 38 Followers: 41,305</p> <p>Network Origin: Poland Description: We assess that this network operated from Poland and targeted a Polish audience. The individuals behind this network created inauthentic accounts in order to make coordinated and directed posts supporting a Polish politician. The network was found to strategically synchronise activity/content across multiple platforms through hashtags and the timing of posts. Accounts Removed: 12 Followers: 10,252</p> <p>Network Origin: Ukraine We assess that this network operated from Ukraine and targeted audiences in Russia, Georgia, Croatia, and Belarus. The individuals behind this network created inauthentic accounts to undermine political candidates favoring Russian-aligned agendas, amplify anti-government protests, and incite ethnic hatred. We assess that the network used off-platform generative artificial intelligence tools in order to create fictitious user avatars. Accounts Removed: 28,713 Followers: 300,456</p> <p>Network Origin: Ukraine Description: We assess that this network operated from Ukraine and targeted a Russian audience. The individuals behind this</p>



	<p>network created inauthentic accounts in order to demoralize the Russian side in the context of the Kursk and Belgorod offensives during the ongoing Russia-Ukraine war. The network was observed to create fictitious personas in order to amplify the reach of its content.</p> <p>Accounts Removed: 32 Followers: 13,940</p> <p>Network Origin: Ukraine Description: We assess that this network operated from Ukraine and targeted audiences in Germany and Ukraine. The individuals behind this network created inauthentic accounts in order to promote anti-Russian viewpoints, within the context of the war between Russia and Ukraine. The network started by targeting a domestic Ukrainian audience but then changed the language used in its videos in order to target a German audience</p> <p>Accounts Removed: 20 Followers: 200,048</p> <p>Network Origin: Russia Description: We assess that this network operated from Russia and targeted Moldovan audiences. The individuals behind the network created inauthentic accounts to deliver content that criticized incumbent Moldovan officials and promoted political figures sympathetic to Russian foreign policy on Moldova. The network was found to be using location obfuscation services in order to hide their true location.</p> <p>Accounts Removed: 314 Followers: 108,823</p> <p>Network Origin: Russia We assess that this network operated from Russia and targeted a European audience. The individuals behind this network created inauthentic accounts posing as journalists from established European news agencies in order to amplify narratives undermining Moldova's government and Moldova's European Union candidate status. The network was found to be using location obfuscation services in order to hide its true operating location.</p> <p>Accounts Removed: 116 Followers: 4,372</p> <p>We published this information within our most recently published transparency report here.</p>
<p>Tackling synthetic and manipulated media</p> <p>(Commitments 14 and 15, Measures 14.1, 15.1 and 15.2).</p>	<p>Description of intervention</p> <p>Artificial intelligence (AI) enables incredible creative opportunities, but can potentially confuse or mislead users if they're not aware content was generated or edited with AI.</p>



	<p>Our 'Edited Media and AI-Generated Content (AIGC)' policy became effective in May 2024. In this policy we prohibit AIGC showing fake authoritative sources or crisis events, or falsely showing public figures in certain contexts, including being bullied, making an endorsement, or being endorsed. TikTok has also started to automatically label AIGC when it's uploaded from certain other platforms.</p> <p>For the purposes of our policy, AIGC refers to content created or modified by artificial intelligence (AI) technology or machine-learning processes, which may include images of real people, and may show highly realistic-appearing scenes, or use a particular artistic style, such as a painting, cartoons, or anime. 'Significantly edited content' is content that shows people doing or saying something they did not do or say, or altering their appearance in a way that makes them difficult to recognise or identify.</p> <p>In accordance with our policy, we prohibit AIGC that features:</p> <ul style="list-style-type: none"> • The likeness of young people or realistic-appearing people under the age of 18 that poses a risk of sexualization, bullying, or privacy concerns, including those related to personally identifiable information or likeness to private individuals • The likeness of adult private figures, if we become aware it was used without their permission • Misleading AIGC or edited media that falsely shows: <ul style="list-style-type: none"> ○ Content made to seem as if it comes from an authoritative source, such as a reputable news organisation ○ A crisis event, such as a conflict or natural disaster ○ A public figure who is: <ul style="list-style-type: none"> ■ being degraded or harassed, or engaging in criminal or antisocial behaviour ■ taking a position on a political issue, commercial product, or a matter of public importance (such as an elections) ■ being politically endorsed or condemned by an individual or group <p>As AI evolves, we continue to invest in combating harmful AIGC by evolving our proactive detection models, consulting with experts, and partnering with peers on shared solutions.</p> <p>Prohibited practices are set out in our Integrity and Authenticity policies here.</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 War in Ukraine and more broadly on our platform.</p>
--	---



<p>Removing harmful misinformation from our platform</p> <p>(Commitment 14, Measure 14.1)</p>	<p>Description of intervention</p> <p>We take action to remove accounts or content that contain inaccurate, misleading, or false content 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 that makes false and harmful claims about specific events, or incites panic. In certain circumstances, we may also reduce the prominence of such content where it does not warrant removal.</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 to remove harmful misinformation that violates our policies before it is reported to us by users or third parties.</p> <p>We place significant emphasis on proactive content moderation at TikTok, and are proud that we remove the vast majority of violative videos before they are reported to us by users or other 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><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 - 3,405 • Number of videos not recommended because of violation of misinformation policy with a proxy (only focusing on RU/UA) - 5,299 • Number of proactive removals of videos removed because of violation of misinformation policy with a proxy related to the War in Ukraine - 3,110
<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>(Commitment 18, Measure 18.1)</p>	<p>Description of intervention</p> <p>TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>N/A</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 strengthened our state-affiliated media policy in order to provide context to users 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 media outlets and accounts subject to sanctions.</p> <p>We continue to strive to update our state-affiliated media policy in order to strengthen our approach to countering influence attempts. Recent updates included:</p> <ul style="list-style-type: none"> • Prohibiting state-affiliated media accounts attempting to engage in foreign influence campaigns from advertising outside of the country with which they are primarily affiliated; including in the EU • Investing in our detection capabilities of state-affiliated media accounts; AND <p>We have also worked with third-party external experts to shape our state-affiliated media policy and assessment of state-controlled media labels.</p> <p>Where our state-affiliated media label is applied to content posted by the accounts of such entities in Russia, Ukraine, and Belarus, users across the EEA are automatically shown a full screen pop-up containing 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>In addition to the above, we continue to invest in automation and scaled detection of state-affiliated media accounts. We also continue to work with third-party experts who help shape our state-affiliated media policies and who help inform our assessments of accounts that have been labelled as state-controlled. We continue to improve our existing processes for applying our state-affiliated media label, such as looking to automate where possible, and aiming to streamline all communications to ensure maximum efficiency. We also continue our efforts in developing an additional layer of intervention to state-affiliated accounts that engage in harmful behaviours.</p>



	<p><i>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</i></p> <p>We continue the detection and labelling of state-controlled media accounts in accordance with our state-controlled media label policy globally.</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 - 13,847 • Number of impressions of the state-affiliated media label for Russia, Belarus, and Ukraine - 100,813,065
<p>Creating localised media literacy campaigns</p> <p><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 that are aimed at improving our users' digital literacy and increasing the prominence of authoritative information.</p> <p>We have localised media literacy campaigns related to the crisis to raise awareness amongst our users. We promoted the campaign through a combination of our in-app intervention tools to ensure that authoritative information is promoted to our users. We have also partnered with a local Ukrainian fact-checking organisation, VoxCheck, with the aim of launching a permanent media literacy campaign in Ukraine.</p> <p>Users searching for keywords related to the War in Ukraine are directed to tips, prepared in partnership with our fact checking partners. These tips help users identify misinformation and prevent its spread 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, we have 17 localised media literacy campaigns addressing disinformation related to the War in Ukraine in Austria, Bosnia, Bulgaria, Czech Republic, Croatia, Estonia, Germany, Hungary, Latvia, Lithuania, Montenegro, Poland, Romania, Serbia, Slovakia, Slovenia, and Ukraine.</p> <p><i>Relevant metrics for the media literacy campaigns (EEA total numbers):</i></p> <ul style="list-style-type: none"> • Total Number of impressions of the search intervention - 30,442,000 • Total Number of clicks on the search intervention - 155,726 • Click through rate of the search intervention - 0.51%



Empowering the Research Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Measures taken to support research into crisis related misinformation and disinformation (Commitment 26, Measure 26.1 and 26.2)	Description of intervention 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 from our platform. More information is available here .
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available During the period of this COCD report, we approved 2 applications through the Research API, with an express focus on the War in Ukraine.
Empowering the Fact-Checking Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Applying our unverified content label and making content ineligible for recommendation (Commitment 31, Measure 31.2)	Description of intervention 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.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available 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 Community Guidelines.



	<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>(Commitment 30, Measure 30.1)</p>	<p>Description of intervention</p> <p>Our fact checking efforts cover Russian, Ukrainian, Belarusian and all major European languages (including 18 official European languages as well as a number of other languages which affect European users).</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>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 12 fact-checking partners in Europe, covering the spoken language of 25 languages (22 official EU languages plus Russian, Ukrainian, and Turkish). One of our fact-checking partners, Reuters, is dedicated to helping us to accurately fact-check 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><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 - 881 • Number of videos removed as a result of a fact-checking assessment with words related to the War in Ukraine - 144 • Number of videos not recommended in the For Your Feed as a result of a fact-checking assessment with words related to the War in Ukraine - 323
<p>Collaborating with our fact-checking partners in relation to emerging</p>	<p>Description of intervention</p> <p>TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document</p>

trends (Commitment 31, Measure 31.1)	<i>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</i> N/A
---	--

Reporting on the service's response during a crisis

Israel - Hamas Conflict

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

TikTok acknowledges both the significance and sensitivity of the Israel-Hamas conflict (referred to as the “Conflict” throughout this section). We understand this remains a difficult, fearful, and polarizing time for many people around the world and on TikTok. TikTok continues to recognise the need to engage in content moderation of violative content at scale while ensuring that the fundamental rights and freedoms of European citizens are respected and protected. We remain dedicated to 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 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 during the reporting period.

(I) Spread of harmful misinformation

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 and Authenticity policies](#) (Integrity and Authenticity policies) in our [Community Guidelines](#); products; practices; and 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.

We continue to take swift action against misinformation, conspiracy theories, fake engagement, and fake accounts relating to the Conflict.

(II) Covert Influence Operations (CIO)

TikTok's integrity and authenticity 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 disrupting CIO networks has been a high priority for us in the context of the Conflict. We now provide regular updates on the CIO networks we detect and remove from our platform, including those we identify relating to the Conflict, in our dedicated [CIO transparency report](#). Between January to June 2025, we reported one new CIO network disruption that was found to post content relating to the Conflict as a dominant theme.

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.

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 global team of thousands 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. In H1 2025, we have removed 7,589 videos in relation to the conflict, which violated our misinformation policies.

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 that violates 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

TikTok has Arabic and Hebrew speaking moderators in the content moderation teams who review content and assist 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, between January to June 2025, we took action to remove one network (consisting of twelve accounts in total) that were found to be related to the Conflict. We now publish all of the CIO networks we identify and remove, including those relating to the conflict, within our dedicated CIO transparency report, [here](#).

(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](#), GPPPA labelling, and [safety and civility policies](#) help to mitigate the risk of monetisation of harmful misinformation.

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

To help raise awareness and to protect our users, we previously 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. In H2 2024 we continued to refine this process; in particular, we focused on improving keywords to ensure they are relevant and effective.

(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
		<p>We refined and expanded our newsworthy exceptions to allow the dissemination of content documenting from a conflict zone and legitimate political speech/criticism, while remaining sensitive to the potential harm users may experience from exposure to graphic visuals, hateful behaviours, or incitement to violence. As part of this effort, we introduced dedicated policies addressing content related to the Conflict, specifically in areas depicting hostages, human suffering, and protests.</p> <p>Additionally, we strengthened our policies on content that glorifies Hamas or Hezbollah and on the promotion or celebration of violent acts committed by either side of the Conflict. To further enhance platform integrity, we implemented specific Integrity and Authenticity policies for Israel-Hamas-related content, with a focus on conspiracy theories of varying severity and unsubstantiated claims.</p>
	We continue to rely on our existing, robust Integrity and Authenticity policies, which are an effective basis for tackling content related to the Conflict. As such, we have not needed to introduce any new	<p>In the context of the Conflict, we rely on our robust Integrity and Authenticity policies as our first line of defence in combating harmful misinformation and deceptive behaviours on our platform.</p> <p>Our Community Guidelines clearly identify to our users what content we remove or make ineligible for the For You feed when it poses 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 Integrity and Authenticity, including within the areas of product and policy. Our experienced subject</p>



	<p>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>matter experts on Integrity and Authenticity 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 Integrity and Authenticity 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 Integrity and Authenticity 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 given the heightened safety risk in the context of the current hostage situation.</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>
Scrutiny of Ads Placements		
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.		
Preventing misuse of our monetisation features	<p><i>Description of intervention</i></p> <p>TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document.</p>	



<p>(Commitment 1, Measure 1.1 and 1.4)</p>	<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. These policies prohibit, among other things, ad content and landing pages to display negative content regarding the military or police symbols, sensitive military events, militarism, advocating or whitewashing of war, terrorism, illegal organizations, or unlawful elements.</p> <p>We've continued to invest in both automated moderation technology, which now takes down 80% of the content removed from TikTok, as well as moderators. We've continued to update and expand our hate speech policy refreshers, trainings, and course materials, including implicit bias training addressing antisemitism and Islamophobia. We also had additional training from the Anti-Defamation League and the American Jewish Committee to further our understanding of new threats facing the Jewish community.</p> <p>Our Monetisation Integrity department has moderation teams in multiple locations that speak Arabic and Hebrew.</p>
	<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</p>	<p>Description of intervention</p> <p>TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document</p>



(Commitment 5, Measure 5.1)	<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>(Commitment 14, Measure 14.1)</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 Integrity and Authenticity 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 that are on high alert to investigate and detect CIO networks on our platform and have removed networks targeting discourse about the Conflict, in accordance with our Integrity and Authenticity 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 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>Between January to June 2025, we took action to remove the following network (consisting of 12 accounts in total) that were found to be related to the Conflict:</p> <p>Network Origin: US Description: We assess that this network operated from the US and targeted a domestic US audience. The individuals behind the network created inauthentic accounts in order to artificially amplify narratives critical of Israel and US support of Israel. The network inflated its reach by frequently reposting, liking, and commenting on content published by other network accounts. Accounts in network: 12 Followers of network: 26,647</p>



	<p>We now publish all of the CIO networks we identify and remove, including those relating to the Conflict, within our dedicated CIO transparency report, 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>Our Edited Media and AI-Generated Content (AIGC) policy makes it clear that we do not want our users to be misled about crisis events. For the purposes of our policy, AIGC refers to content created or modified by AI technology or machine-learning processes. It includes images of real people and may show highly realistic-appearing scenes.</p> <p>We do not allow misleading AIGC or edited media that falsely shows:</p> <ul style="list-style-type: none"> • Content made to seem as if it comes from an authoritative source, such as a reputable news organisation, • A crisis event, such as a conflict or natural disaster, • A public figure who is: <ul style="list-style-type: none"> ○ being degraded or harassed, or engaging in criminal or anti-social behavior ○ taking a position on a political issue, commercial product, or a matter of public importance (such as an election) ○ spreading misinformation about matters of public importance <p>In addition, all AIGC or edited media, including that which depicts public figures, such as politicians, must be clearly labelled as AI-generated, and can not be used for endorsements.</p> <p>We have an AI-generated content label for users to easily inform their community when they post AIGC. 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 AIGC that shows realistic scenes. Creators can do this through this label or through other types of disclosures, like a sticker, watermark, or caption.</p> <p>TikTok is also proud to be a part of, the Content Authenticity Initiative (CAI) and the Coalition for Content Provenance and Authenticity (C2PA), and were the first video sharing platform to put Content Credentials into practice. TikTok has the ability to read Content Credentials that attach metadata to content, which we can use to instantly recognize and label AIGC. This helps our auto-labelling functionality for AIGC created on some other platforms.</p>
	<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, which are relevant both in the context of the Conflict and more broadly on our platform.</p>



<p>Removing harmful misinformation from our platform</p> <p><i>(Commitment 14, Measure 14.1)</i></p>	<p>Description of intervention</p> <p>We employ a dynamic 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 that violates our policies before it is reported to us by users or third parties.</p> <p>We take action to remove accounts or content that 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 that makes false and harmful claims about specific events, or incites panic. In certain circumstances, we may reduce the prominence of such content.</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 have proactively removed 7,177 videos in H1 containing harmful misinformation related to the Conflict. We have been able to do this through a combination of automation and human moderation. We carry 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 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) - 7,589 • Number of videos not recommended because of violation of misinformation policy with a proxy (IL/Hamas) - 14,103 • Number of proactive removals of videos removed because of violation of misinformation policy with a proxy (IL/Hamas): 7,177
<p>Empowering Users</p>	
<p>Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.</p>	
<p>Deploying search</p>	<p>Description of intervention</p>



interventions to raise awareness of potential misinformation <i>(Commitment 21, Measure 21.1)</i>	<p>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). We continuously evaluate the effectiveness of our keywords, adding or removing terms based on their relevance.</p>
	<p><i>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</i></p> <p>These search interventions remind users to pause and check their sources and also direct them to well-being resources.</p>
Not proactively promoting news-type content to our users <i>(Commitment 18, Measure 18.1)</i>	<p><i>Description of intervention</i></p> <p>TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document</p>
	<p><i>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</i></p> <p>N/A</p>
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 Conflict- related misinformation and disinformation <i>(Commitment 26, Measure 26.1 and 26.2)</i>	<p><i>Description of intervention</i></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 from our platform. More information is available here.</p>
	<p><i>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</i></p> <p>Between January and June 2025, 2 Research API applications related to the Conflict have been approved.</p>
Empowering the Fact-Checking Community	



Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Applying our unverified content label to make content ineligible for recommendation <i>(Commitment 31, Measure 31.2)</i>	Description of intervention Where our misinformation moderators or fact-checking partners determine that content cannot 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
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available 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 that may potentially be misleading, we apply our unverified content label to inform users that 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). Where the label 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.
Ensuring fact-checking coverage <i>(Commitment 30, Measure 30.1)</i>	Description of intervention As part of our fact-checking program, TikTok works with more than 20 IFCN-accredited fact-checking organisations that support more than 60 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 Community Guidelines. 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. 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. We also continue to improve our



	<p>hate speech detection with an improved audio hash bank to help detect hateful sounds as well as updated machine learning models to recognize emerging hateful content.</p>
	<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 - 1,913 • Number of videos removed as a result of a fact checking assessment with words related to IL/Hamas - 242 • Number of videos demoted (NR) as a result of a fact checking assessment with words related to IL/Hamas - 323
<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>TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>N/A</p>



Reporting on the signatory's response during an election

Polish Election 2025

Threats observed during the electoral period: [suggested character limit 2000 characters].

The 2025 Polish Presidential Election was a high-risk election with significant negative exposure potential. Round 1 elections occurred on 18 May, and the run-off was held on 1 June. Official results were announced on 2 June. Because of its significance in the context of Poland's domestic policies and international relations, we activated our Mission Control Centre (MCC) work in advance of the election, which resulted in identifying and containing threats early and quickly. Regulators publicly praised TikTok's collaboration, and national media highlighted TikTok "more ambitious" safety posture compared to rival platforms. Some examples of the violative content we successfully disrupted include:

- **Content removals:** We proactively removed more than 3,300 pieces of election-related content in Poland for violating our policies on synthetic and manipulated media, misinformation, and civic and election integrity.
- **Covert influence disruption:** We removed three new domestic CIO networks (totaling 77 accounts and 36,419 followers) that were identified as specifically targeting a Polish audience for manipulating election discourse using fake news accounts and personas. More information relating to network disruptions is published on our dedicated [Covert Influence Operations Reports](#).

Mitigations in place during the electoral period: [suggested character limit: 2000 characters].

Enforcing our policies

(I) Moderation capabilities

We have thousands of trust and safety professionals dedicated to keeping our platform safe. As they usually do, our teams worked alongside technology to ensure that we were consistently [enforcing our rules](#) to detect and remove misinformation, covert influence operations, and other content and behaviour that can increase during an election period. In advance of the election we had proactive data monitoring, trend detection and regular monitoring of enriched keywords and accounts.

(II) Mission Control Centre: internal cross-functional collaboration

TikTok established a Mission Control Centre (MCC) in advance of the election, developed risk scenario mapping (covering focused Russian influence operations, AI-generated content (AIGC), misinformation/disinformation, scaled inauthentic behavior, hate speech surges), and implemented regular content



trend clustering with rolling containment-correction-and-prevention cycle, covering key features. As a result, all identified threats were contained or mitigated early, with no credible or substantiated election interference claims emerging.

(III) Countering misinformation

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.

In the weeks leading up to and including the run-off, we removed **530** videos for violating our civic and election integrity policies, and **2,772** videos for violating our misinformation policies.

(IV) Fact-checking

Our global fact-checking programme is a critical part of our layered approach to detecting harmful misinformation in the context of elections. The core objective of the fact-checking program is to leverage the expertise of external fact-checking organisations to help assess the accuracy of potentially harmful claims that are difficult to verify.

Within Europe, we partnered with 12 fact-checking organisations who provide fact-checking coverage in 25 languages (22 official EU languages plus Russian, Ukrainian and Turkish). [Demagog](#), serves as the fact-checking partner for Poland, which provides coverage for the platform.

(V) Deterring covert influence operations

We prohibit covert influence operations and remain constantly vigilant against attempts to use deceptive behaviours and manipulate our platform. We proactively seek and continuously investigate leads for potential influence operations. We're also working with government authorities and encourage them to share any intelligence so that we can work together to ensure election integrity. More detail on our policy against covert influence operations is published on our [website](#).

(VI) Tackling misleading AI-generated content

Creators are required to label any realistic AI-generated content (AIGC) and we have an [AI-generated content label](#) to help people do this. TikTok has a 'Edited Media and AI-Generated Content (AIGC)' policy, which prohibits AIGC showing fake authoritative sources or crisis events, or falsely showing public figures in certain contexts including being bullied, making an endorsement, or being endorsed.

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



Many political leaders, ministers, and political parties have a presence on TikTok. 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.

We strongly recommend GPPAs have their accounts [verified by TikTok](#). Verified badges help users make informed choices about the accounts they choose to follow. It is 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.

Directing people to trusted sources

(I) Investing in media literacy

We invest in media literacy campaigns as a counter-misinformation strategy, working with fact checkers as part of our Election Centre for Poland. TikTok has partnered with Demagog and [FakeNews.pl](#) in Poland to help the community safely navigate the platform and protect themselves against potential misinformation during the elections. We also worked with fact checkers to launch an Evergreen Media Literacy Campaign.

External engagement at the national and EU levels

(I) Rapid Response System: external collaboration with COPD Signatories

The COCD Rapid Response System (RRS) was utilised to exchange information among civil society organisations, fact-checkers, and online platforms. TikTok received 23 RRS reports through the RRS before the Polish Election, which were rapidly addressed, including [NASK](#) and DSA cases. Actions included banning of accounts and content removals for violation of Community Guidelines.

(II) Engagement with local experts

To further promote election integrity, and inform our approach to the Polish Election, we organised an Election Speaker Series with Demagog who shared their insights and market expertise with our internal teams.

[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
N/A	N/A	
Scrutiny of Ads Placements		
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.		
Scrutiny of Ad Placements, including prohibition on monetisation and fundraising campaigns for GPPAs (Commitment 1 and Measure 1.1)	Description of intervention TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document	
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available N/A	
Political Advertising		
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.		
Prohibition on Political Advertising (Commitment 5, Measure 5.1)	Description of intervention TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document	



	Indication of impact (at beginning of action: expected impact) including relevant metrics when available N/A
Integrity of Services	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Identifying and removing CIO networks (Commitment 14, Measure 14.1)	<p style="text-align: center;">Description of intervention</p> <p>During the Polish Election we continued our work to detect and disrupt covert influence operations (CIOs) that attempt to establish themselves on TikTok and undermine the integrity of our platform. To further increase transparency, accountability, and cross-industry sharing we introduced dedicated covert influence operations reports.</p> <p>Accounts targeting political discourse in Poland We assess that this network operated from Poland and targeted a Polish audience. The individuals behind this network created inauthentic accounts in order to promote nationalistic viewpoints that criticized Poland's engagement with the EU and aid to Ukraine, within the context of the 2025 Polish presidential election. The network systematically recycled content throughout its accounts in order to further spread its messaging.</p> <ul style="list-style-type: none"> ● Removed accounts in network: 16 ● Followers of Network: 14,743 <p>We assess that this network operated from Poland and targeted a Polish audience. The individuals behind this network created inauthentic accounts in order to make coordinated and directed posts supporting a Polish politician. The network was found to strategically synchronise activity/content across multiple platforms through hashtags and the timing of posts.</p> <ul style="list-style-type: none"> ● Removed accounts in network: 12 ● Followers of Network: 10,252 <p>We assess that this network operated from Poland and targeted a Polish audience. The individuals behind this network created inauthentic accounts in order to discredit the current government within the context of the 2025 Polish presidential election. The network was found to post videos that exploited the Volhynia Massacre and other sensitive historical topics to promote Eurosceptic, anti-Ukrainian, and anti-Semitic narratives.</p>



	<ul style="list-style-type: none"> ● Removed accounts in network: 49 ● Followers of Network: 11,424 <p>More information relating to the above detailed network disruptions is published on our dedicated Covert Influence Operations transparency page.</p>
Tackling misleading AIGC and edited media <i>(Commitment 15, Measures 15.1 and 15.2)</i>	<p style="text-align: center;">Description of intervention</p> <p>Our Edited Media and AI-Generated Content (AIGC) policy makes it clear that we do not want our users to be misled about political issues. For the purposes of our policy, AIGC refers to content created or modified by artificial intelligence (AI) technology or machine-learning processes, which may include images of real people, and may show highly realistic-appearing scenes, or use a particular artistic style, such as a painting, cartoons, or anime.</p> <p>We do not allow misleading AIGC or edited media that falsely shows:</p> <ul style="list-style-type: none"> ● Content made to seem as if it comes from an authoritative source, such as a reputable news organisation, ● A crisis event, such as a conflict or natural disaster, ● A public figure who is: <ul style="list-style-type: none"> ○ being degraded or harassed, or engaging in criminal or anti-social behaviour ○ taking a position on a political issue, commercial product, or a matter of public importance (such as an elections) ○ being politically endorsed or condemned by an individual or group. <p>In addition, all AIGC or edited media, including that which depicts public figures, such as politicians, must be clearly labelled as AI generated, and can not be used for endorsements.</p> <p>As AI evolves, we continue to invest in combating harmful AIGC by evolving our proactive detection models, consulting with experts, and partnering with peers on shared solutions.</p> <p>TikTok has invested in labeling technologies and tools, including the implementation of Content Credentials technology from the Coalition for Content Provenance and Authenticity (C2PA), which enables the automatic recognition and labeling of AI-generated content. This is complemented by a TikTok-developed tool that allows creators to easily label AI-generated</p>



	<p>content, already used by 37 million creators. TikTok's commitment to AIGC transparency ensures a safe environment for users, who can easily identify synthetic content and understand its context.</p> <p>TikTok is a member of the Content Authenticity Initiative and the Coalition for Content Provenance and Authenticity, and was the first video sharing platform to put Content Credentials into practice. We have the ability to read Content Credentials that attach metadata to content, which we can use to instantly recognise and label AIGC. This helped us to expand auto-labelling to AIGC created on some other platforms.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>Number of videos removed because of violation of our Edited media and AIGC policy from 21-27 April to 26 May to 1 June to cover both rounds of the Polish Elections and four complete weeks preceding Round 1: 75</p>
Empowering Users	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Rolling out Media literacy campaigns <i>(Commitment 17, Measure 17.2)</i>	<p>Description of intervention</p> <p>From 18 April 2025, Tiktok launched an in-app Election Centre to provide users with up-to-date information about the 2025 Polish election. Working with electoral commissions and civil society organisations, the Election Centre connected people with reliable voting information, including when, where, and how to vote; eligibility requirements for candidates; and, ultimately, the election results.</p> <p>The Election Centre contained a section about spotting misinformation, which included videos created in partnership with our fact-checking partner Demagog, fact checker FakeNews.pl, and media partners Radio Zet and Orientuj.sie. We directed people to the Election Centre through prompts on videos, LIVES and searches related to elections.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>The Election Centre launched before the Polish Election was visited 1,968,010 times.</p>
Engagement with local and regional experts	<p>Description of intervention</p>



<p>(Commitment 17, Measure 17.2)</p>	<p>To further promote election integrity, and inform our approach to the Polish Election, we organised an Election Speaker Series with Demagog who shared their insights and market expertise with our internal teams.</p> <p>Our fact-checking partners and local media literacy bodies have also supported TikTok in our launch of the Election Centres, which featured videos from them. This localised approach helped to ensure that messaging in relation to the Polish election was relevant to our community and encouraged more engagement.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>This engagement with external regional and local experts allowed us to inform our country-level approach to the Polish Election.</p>
<p>Empowering the Research Community</p>	
<p>Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.</p>	
<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, and comments from our platform. More information is available here.</p> <p>We conduct regular workshops for researchers, both online and in-person, to facilitate successful applications, provide hands-on demonstrations of our research tools, and address questions. These sessions are designed to maximize researcher success. Since launching January 2025-June 2025, we have delivered over 9 workshops, engaging more than 150 researchers. This included Germany, Romania, Poland, and Czech Republic.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>Number of Research API applications related to the Polish Election that have been approved from January to June 2025: One application was received.</p>



Empowering the Fact-Checking Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Ensuring fact-checking coverage (Commitment 30, Measure 30.1)	Description of intervention
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available
	Demagog , serves as the fact-checking partner for Poland, which provided coverage for the platform.
	Please refer to Chapter 7 - Empowering the Fact-Checking Community for metrics.



Reporting on the signatory's response during an election

German Federal Election 2025

Threats observed during the electoral period: [suggested character limit 2000 characters].

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 German federal election held on 23 February 2025 . In advance of the election, a core election team was formed and consultations between cross function teams helped to identify and design response strategies.

TikTok did not observe major threats during the German election. Some examples of the violative content we successfully disrupted in German during January 2025:

- We removed more than 862,000 pieces of content for violating our Community Guidelines, which includes our policies on [civic and election integrity](#) and [misinformation](#).
- We also removed 712 accounts for impersonating German election candidates and elected officials.
- We proactively prevented +24 million fake likes and +18.9 million fake follow requests. We also blocked +293,000 spam accounts from being created.
- We also removed +700,000 fake accounts, +17 million fake likes, and +5.7 million fake followers.

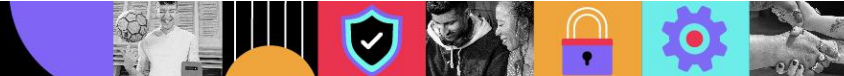
Mitigations in place during the electoral period: [suggested character limit: 2000 characters].

Enforcing our policies

(I) Moderation capabilities

We have thousands of trust and safety professionals dedicated to keeping our platform safe. As they usually do, our teams worked alongside technology to ensure that we were consistently [enforcing our rules](#) to detect and remove misinformation, covert influence operations, and other content and behaviour that can increase during an election period. In advance of the election, we had proactive data monitoring, trend detection and regular monitoring of enriched keywords and accounts.

(II) Mission Control Centre: internal cross-functional collaboration



On 18 November, ahead of the German election, we established a dedicated Mission Control Centre (MCC) bringing together employees from multiple specialist teams within our safety department. Through the MCC, our teams were able to provide consistent and dedicated coverage of potential election-related issues in the run-up to, and during, the election.

(III) Countering misinformation

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.

In January 2025, we removed more than 862,000 pieces of content for violating our Community Guidelines, which includes our policies on [civic and election integrity](#) and [misinformation](#).

In the weeks leading up to and including the election, we removed 3,283 videos for violating our civic and election integrity policies, and 12,781 videos for violating our misinformation policies.

(IV) Fact-checking

Our global fact-checking programme is a critical part of our layered approach to detecting harmful misinformation in the context of elections. The core objective of the fact-checking program is to leverage the expertise of external fact-checking organisations to help assess the accuracy of potentially harmful claims that are difficult to verify.

TikTok collaborates with [12 fact-checking organizations](#) across Europe to evaluate the accuracy of content in most European languages, including German. [Deutsche Presse-Agentur \(dpa\)](#), serves as the fact-checking partner for Germany, which provides coverage for the platform.

(V) Deterring covert influence operations

We prohibit covert influence operations and remain constantly vigilant against attempts to use deceptive behaviours and manipulate our platform. We proactively seek and continuously investigate leads for potential influence operations. We're also working with government authorities and encourage them to share any intelligence so that we can work together to ensure election integrity. More detail on our policy against covert influence operations is published on our [website](#) as well as monthly [Covert Influence Operations reports](#).

(VI) Tackling misleading AI-generated content

Creators are required to label any realistic AI-generated content (AIGC) and we have an [AI-generated content label](#) to help people do this. TikTok has a 'Edited Media and AI-Generated Content (AIGC)' policy, which prohibits AIGC showing fake authoritative sources or crisis events, or falsely showing public figures in certain contexts including being bullied, making an endorsement, or being endorsed.



(VII) Government, Politician, and Political Party Accounts (GPPPs)

Many political leaders, ministers, and political parties have a presence on TikTok. 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.

We strongly recommend GPPPs have their accounts [verified by TikTok](#). Verified badges help users make informed choices about the accounts they choose to follow. It is 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.

Before the German election, we provided all parties represented in federal and state parliaments with written information about our election integrity policies and measures, and offered virtual information sessions for the parties and their candidates. We presented at security-focused webinar for candidates and parties organised by the Federal Office for Information Security (BSI). We also offered all parties represented in federal and state parliaments verification support for their candidates.

Directing people to trusted sources

(I) Investing in media literacy

We invest in media literacy campaigns as a counter-misinformation strategy. From 16 Dec 2024 to 3 Mar 2025, we launched an in-app [Election Centre](#) to provide users with up-to-date information about the 2025 German federal election. The centre contained a section about spotting misinformation, which included videos created in partnership with the fact-checking organisation [Deutsche Presse-Agentur \(dpa\)](#). The Election Center was visited more than 5.7 million times.

External engagement at the national and EU levels

(I) Rapid Response System: external collaboration with COPD Signatories

The COPD Rapid Response System (RRS) was utilised to exchange information among civil society organisations, fact-checkers, and online platforms. TikTok received 4 RRS reports through the RRS before the German election which were rapidly addressed. Actions included banning of accounts and content removals for violation of Community Guidelines.

(II) Engagement with local experts

To further promote election integrity, and inform our approach to the German Election, we organised an Election Speaker Series with dpa who shared their insights and market expertise with our internal teams



(III) Engagement with national authorities and stakeholders

We participated in the two election roundtables hosted by the Federal Ministry of the Interior (BMI), one before and one after the election.

We participated in the election roundtable as well as the stress test hosted by the Federal Network Agency (BNetzA), the German Digital Service Coordinator (DSC). In addition, we held three separate virtual meetings between TikTok and the BNetzA, also attended by the European Commission, and answered a set of written questions.

We met with the domestic intelligence service (BfV) and the BMI state secretary.

We attended two election-focused virtual meetings with BzKJ (Federal Agency for Child and Youth Protection) and other platforms.

We engaged with the electoral commissioner ("Bundeswahlleiterin") and onboarded them to TikTok. In our election center, we included 2 videos from the electoral commissioner and linked to their website.

We provided all parties represented in federal and state parliaments with information about our election integrity measures and what they/their candidates can and cannot do on the platform in written form and also offered virtual info sessions for the parties and their candidates. We also offered all parties represented in federal and state parliaments verification support for their candidates.

We presented a security-focused webinar for candidates and parties organised by the Federal Office for Information Security (BSI).

[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
N/A	N/A	



Scrutiny of Ads Placements	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Scrutiny of Ad Placements, including prohibition on monetisation and fundraising campaigns for GPPAs <i>(Commitment 1 and Measure 1.1)</i>	Description of intervention TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available N/A
Political Advertising	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Prohibition on Political Advertising <i>(Commitment 5, Measure 5.1)</i>	Description of intervention TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available N/A
Integrity of Services	



Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Identifying and removing CIO networks <i>(Commitment 14, Measure 14.1)</i>	Description of intervention
	<p>During the German election we continued our work to detect and disrupt covert influence operations (CIOs) that attempt to establish themselves on TikTok and undermine the integrity of our platform. To further increase transparency, accountability, and cross-industry sharing, we introduced dedicated covert influence operations reports.</p>
Tackling misleading AIGC and edited media <i>(Commitment 15, Measures 15.1 and 15.2)</i>	Indication of impact (at beginning of action: expected impact) including relevant metrics when available
	<p>In February 2025, we disrupted three small scale covert influence operations targeting the German market within the context of the federal election:</p> <ol style="list-style-type: none"> 1. A network of 40 accounts operated from Germany and targeted a German audience. The individuals behind this network created inauthentic accounts in order to amplify content supporting the political party "Alternative for Germany (AfD)." A large proportion of the network's accounts were found to use the word "news" or "nachricht" in their handle or nickname. 2. A network of 17 accounts operated from Germany and targeted a German audience. The individuals behind this network created inauthentic accounts in order to promote the "Bündnis Sahra Wagenknecht (BSW)" Party within the context of the 2025 German federal elections. The network was found to alternate between posting apolitical and political content in order to drive engagement. 3. A network of 14 accounts operated from Germany and targeting a German audience. The individuals behind this network created inauthentic accounts in order to promote the political party "Alternative for Germany (AfD)". The accounts used Smurf avatars and were observed to rebrand their accounts and alternate content in order to gain engagement. <p>In addition to these network disruptions, we continued to remove accounts associated with previously disrupted networks attempting to re-establish their presence within this reporting period.</p>
	Description of intervention
	<p>Our Edited Media and AI-Generated Content (AIGC) policy makes it clear that we do not want our users to be misled about political issues. For the purposes of our policy, AIGC refers to content created or modified by artificial intelligence (AI) technology or machine-learning processes, which may include images of real people, and may show highly realistic-appearing scenes, or use a particular artistic style, such as a painting, cartoons, or anime.</p>



	<p>We do not allow misleading AIGC or edited media that falsely shows:</p> <ul style="list-style-type: none"> • Content made to seem as if it comes from an authoritative source, such as a reputable news organisation, • A crisis event, such as a conflict or natural disaster, • A public figure who is: <ul style="list-style-type: none"> ○ being degraded or harassed, or engaging in criminal or anti-social behaviour ○ taking a position on a political issue, commercial product, or a matter of public importance (such as an elections) ○ being politically endorsed or condemned by an individual or group. <p>In addition, all AIGC or edited media, including depictions of public figures, such as politicians, must be clearly labelled as AI generated, and can not be used for endorsements.</p> <p>As AI evolves, we continue to invest in combating harmful AIGC by evolving our proactive detection models, consulting with experts, and partnering with peers on shared solutions.</p> <p>TikTok has invested in labeling technologies and tools, including the implementation of Content Credentials technology from the Coalition for Content Provenance and Authenticity (C2PA), which enables the automatic recognition and labeling of AI-generated content. This is complemented by a TikTok-developed tool that allows creators to easily label AI-generated content, already used by 37 million creators. TikTok's commitment to AIGC transparency ensures a safe environment for users, who can easily identify synthetic content and understand its context.</p> <p>TikTok is a member of the Content Authenticity Initiative and the Coalition for Content Provenance and Authenticity, and was the first video sharing platform to put Content Credentials into practice. We have the ability to read Content Credentials that attach metadata to content, which we can use to instantly recognise and label AIGC. This helped us to expand auto-labelling to AIGC created on some other platforms.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>Number of videos removed for violating our Edited Media and AIGC policy during the 4 weeks leading up to and including the day of the German federal election on 23 February 2025: 574</p>
Empowering Users	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	

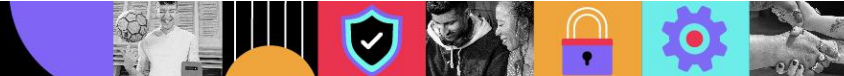


Rolling out Media literacy campaigns <i>(Commitment 17, Measure 17.2)</i>	Description of intervention <p>In advance of EU and select regional elections, TikTok works with electoral commissions, civil society organisations, and fact-checking bodies to establish in-app Election Centres that connect people with reliable voting information, including: when, where, and how to vote; eligibility requirements for candidates; and, ultimately, the election results. We direct people to the Election Centres through prompts on videos, LIVES and searches related to elections.</p> <p>From 16 Dec 2024 to 3 Mar 2025, we had a dedicated in-app Election Centre providing users with up-to-date information about the German federal election. The centre contained a section about spotting misinformation, which included videos created in partnership with our fact-checking partner Deutsche Presse-Agentur (dpa). On 21 February 2025, we also launched a new permanent general media literacy and critical thinking skills campaign in Germany in collaboration with Deutsche Presse-Agentur (dpa). During H1 2025, we further enhanced awareness and visibility about how we tackle election misinformation and covert influence operations on our platform through the launch of our Global Elections Hub. This evergreen resource provides users and external stakeholders with timely updates on our election integrity efforts throughout each election cycle.</p>
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available <p>The Election Centre launched in advance of the German federal election was visited 5,708,749 times, and search banners were viewed 712,652 times. This localised approach helped to ensure that messaging in relation to the election was relevant to our community and encouraged more engagement.</p>
Engagement with local and regional experts <i>(Commitment 17, Measure 17.2)</i>	Description of intervention <p>To further promote election integrity, and inform our approach to the election, we organised an Election Speaker Series on 14 January 2025 with Deutsche Presse-Agentur (dpa) who shared their insights and market expertise with our internal teams.</p>
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available <p>This engagement with external regional and local experts allowed us to inform our country-level approach to the German election.</p>
Empowering the Research Community	



Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Providing access to our Research API <i>(Commitment 26 and Measures 26.1 and 26.2)</i>	Description of intervention To make it easier to independently research our platform and bring transparency to TikTok content, we built a Research API that provides researchers in the US, EEA, UK and Switzerland, with access to public data on accounts and content, including comments, captions, subtitles, number of comments, shares, likes, followers and following lists, and favourites that a video receives on our platform. More information is available here .
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available Number of Research API applications related to the German federal election that were approved in H1 2025: 15
Empowering the Fact-Checking Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Ensuring fact-checking coverage <i>(Commitment 30, Measure 30.1)</i>	Description of intervention Deutsche Presse-Agentur (dpa) serves as the fact-checking partner for Germany , which provides coverage for the platform.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available Please see Chapter VII for relevant metrics.

Reporting on the signatory's response during an election
Portuguese Election 2025
Threats observed during the electoral period: [suggested character limit 2000 characters].



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 Portugal legislative election held on 18 May 2025. In advance of the election, a core election team was formed and consultations between cross function teams helped to identify and design response strategies.

TikTok did not observe major threats during the Portuguese election. Through the election, we monitored for and actioned inauthentic behavior, and removed content that violated our Community Guidelines. As part of these efforts:

- Between May 12 and May 25, we removed more than 300 pieces of content for violating our policies on [civic and election integrity](#), [misinformation](#) and [AI generated content](#). We removed more than 94% of it before anyone told us about it.
- Between May 12 and 25, we proactively prevented more than 1,800,000 fake likes and more than 671,000 fake follow requests, and blocked more than 5,400 spam accounts from being created in Portugal. We also removed more than 5,400 fake accounts, more than 880,000 fake likes, and more than 154,000 fake followers.
- Between May 15 - May 29, we also removed 28 accounts for impersonating Portuguese election candidates and elected officials.

Mitigations in place during the electoral period: [suggested character limit: 2000 characters].

Enforcing our policies

(I) Moderation capabilities

We have thousands of trust and safety professionals dedicated to keeping our platform safe. As they usually do, our teams worked alongside technology to ensure that we were consistently [enforcing our rules](#) to detect and remove misinformation, covert influence operations, and other content and behaviour that can increase during an election period. In advance of the election, we had proactive data monitoring, trend detection, and regular monitoring of enriched keywords and accounts.

(II) Mission Control Centre: internal cross-functional collaboration

On 13 May, ahead of the Portuguese election, we established a dedicated Mission Control Centre (MCC) bringing together employees from multiple specialist teams within our safety department. Through the MCC, our teams were able to provide consistent and dedicated coverage of potential election-related issues in the run-up to, and during, the election. .

(III) Countering misinformation

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.



In the weeks leading up to and including the election (April 21 to May 18), we removed 821 pieces of content for violating our policies on [civic and election integrity](#), [misinformation](#), and [AI generated content](#). In this same period, we removed over **99%** of violative misinformation content before it was reported to us.

(IV) Fact-checking

Our global fact-checking programme is a critical part of our layered approach to detecting harmful misinformation in the context of elections. The core objective of the fact-checking program is to leverage the expertise of external fact-checking organisations to help assess the accuracy of potentially harmful claims that are difficult to verify.

TikTok collaborates with [12 fact-checking organizations](#) across Europe to evaluate the accuracy of content in most European languages, including Portuguese. [Poligrafo](#), serves as the fact-checking partner for Portugal, which provides coverage for the platform.

(V) Deterring covert influence operations

We prohibit covert influence operations and remain constantly vigilant against attempts to use deceptive behaviours and manipulate our platform. We proactively seek and continuously investigate leads for potential influence operations. We're also working with government authorities and encourage them to share any intelligence so that we can work together to ensure election integrity. More detail on our policy against covert influence operations is published on our [website as](#) well as monthly [Covert Influence Operations reports](#).

(VI) Tackling misleading AI-generated content

Creators are required to label any realistic AI-generated content (AIGC) and we have an [AI-generated content label](#) to help people do this. TikTok has a 'Edited Media and AI-Generated Content (AIGC)' policy, which prohibits AIGC showing fake authoritative sources or crisis events, or falsely showing public figures in certain contexts including being bullied, making an endorsement, or being endorsed.

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

Many political leaders, ministers, and political parties have a presence on TikTok. 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.

We strongly recommend GPPAs have their accounts [verified by TikTok](#). Verified badges help users make informed choices about the accounts they choose to follow. It is 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.



Before the election we met with the main Portuguese regulatory bodies and political parties' Heads of Communication to (i) provide an overview of TikTok's policies for political accounts, (ii) outline TikTok's approach to election integrity and to data security, (iii) encourage account verification and (iv) enable direct contact to respond to their specific requests.

Directing people to trusted sources

(I) Investing in media literacy

We invest in media literacy campaigns as a counter-misinformation strategy. From 18 Apr 2025 to 2 June 2025, we launched an in-app [Election Centre](#) to provide users with up-to-date information about the 2025 Portugal election. The centre contained a section about spotting misinformation, which included videos created in partnership with our fact-checking partner Poligrafo. TikTok has partnered with Poligrafo in Portugal to help the community safely navigate the platform and protect themselves against potential misinformation during the elections. Poligrafo developed a series of educational videos explaining how users could identify and avoid misinformation, use TikTok's safety features, and critically evaluate content related to the electoral process. The Portuguese community could find the video series with practical advice and useful information about the electoral process in the relevant Election Center.

External engagement at the national and EU levels

(I) Rapid Response System: external collaboration with COPD Signatories

The COCD Rapid Response System (RRS) was utilised to exchange information among civil society organisations, fact-checkers, and online platforms. TikTok received 1 RRS report through the RRS during the Portuguese election, which was quickly addressed and resulted in the reported content being deemed [“FYF Ineligible”](#).

(II) Engagement with local experts

To further promote election integrity, and inform our approach to the Portuguese election, we organised an Election Speaker Series with Poligrafo who shared their insights and market expertise with our internal teams.

(III) Engagement with national authorities and stakeholders

Ahead of the election, our Government Relations team represented TikTok at an official meeting organised by ANACOM with the Portuguese Regulatory Authority for the Media (ERC) and the National Election Commission (CNE). The team also met with the Organization for Security and Cooperation in Europe's Office of Democratic Institutions and Human Rights (OSCE/ODIHR) and in particular, their Election Expert Team (EET) deployed for these elections.



As previously referenced, we also met with Portuguese political parties' Heads of Communication to (i) provide an overview of TikTok's policies for political accounts, (ii) outline TikTok's approach to election integrity and to data security, (iii) encourage account verification and (iv) enable direct contact to respond to their specific requests.		
[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
N/A	N/A	
Scrutiny of Ads Placements		
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.		
Scrutiny of Ad Placements, including prohibition on monetisation and fundraising campaigns for GPPAs <i>(Commitment 1 and Measure 1.1)</i>	Description of intervention	
	TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document Indication of impact (at beginning of action: expected impact) including relevant metrics when available N/A	



Political Advertising	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Prohibition on Political Advertising <i>(Commitment 5, Measure 5.1)</i>	Description of intervention <p>TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document</p>
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available <p>N/A</p>
Integrity of Services	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Identifying and removing CIO networks <i>(Commitment 14, Measure 14.1)</i>	Description of intervention <p>During the Portugal election we continued our work to detect and disrupt covert influence operations (CIOs) that attempt to establish themselves on TikTok and undermine the integrity of our platform. To further increase transparency, accountability, and cross-industry sharing we introduced dedicated covert influence operations reports.</p>
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available <p>In May 2025, we disrupted one small scale covert influence operation targeting the Portuguese market within the context of the legislative election:</p> <ul style="list-style-type: none"> We assess that this network targeted a Portuguese audience. The individuals behind this network created inauthentic accounts in order to promote the Socialist Party and undermine the Social Democratic Party, within the context of the 2025 Portuguese election. This network masked its operating location through advanced operational security.



Tackling misleading AIGC and edited media	Description of intervention
<p><i>(Commitment 15, Measures 15.1 and 15.2)</i></p>	<p>Our Edited Media and AI-Generated Content (AIGC) policy makes it clear that we do not want our users to be misled about political issues. For the purposes of our policy, AIGC refers to content created or modified by artificial intelligence (AI) technology or machine-learning processes, which may include images of real people, and may show highly realistic-appearing scenes, or use a particular artistic style, such as a painting, cartoons, or anime.</p> <p>We do not allow misleading AIGC or edited media that falsely shows:</p> <ul style="list-style-type: none"> • Content made to seem as if it comes from an authoritative source, such as a reputable news organisation, • A crisis event, such as a conflict or natural disaster, • A public figure who is: <ul style="list-style-type: none"> ○ being degraded or harassed, or engaging in criminal or anti-social behaviour ○ taking a position on a political issue, commercial product, or a matter of public importance (such as an elections) ○ being politically endorsed or condemned by an individual or group. <p>In addition, all AIGC or edited media, including depictions of public figures, such as politicians, must be clearly labelled as AI generated, and can not be used for endorsements.</p> <p>As AI evolves, we continue to invest in combating harmful AIGC by evolving our proactive detection models, consulting with experts, and partnering with peers on shared solutions.</p> <p>TikTok has invested in labeling technologies and tools, including the implementation of Content Credentials technology from the Coalition for Content Provenance and Authenticity (C2PA), which enables the automatic recognition and labeling of AI-generated content. This is complemented by a TikTok-developed tool that allows creators to easily label AI-generated content, already used by 37 million creators. TikTok's commitment to AIGC transparency ensures a safe environment for users, who can easily identify synthetic content and understand its context.</p> <p>TikTok is a member of the Content Authenticity Initiative and the Coalition for Content Provenance and Authenticity, and was the first video sharing platform to put Content Credentials into practice. We have the ability to read Content Credentials that attach metadata to content, which we can use to instantly recognise and label AIGC. This helped us to expand auto-labelling to AIGC created on some other platforms.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p>



	Number of videos removed for violating our Edited Media and AIGC policy during the 4 weeks leading up to and including the day of the Portuguese election on 18 May 2025: 11
Empowering Users	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Rolling out Media literacy campaigns <i>(Commitment 17, Measure 17.2)</i>	Description of intervention <p>In advance of EU and select regional elections, TikTok works with electoral commissions, civil society organisations, and fact-checking bodies to establish in-app Election Centres that connect people with reliable voting information, including: when, where, and how to vote; eligibility requirements for candidates; and, ultimately, the election results. We direct people to the Election Centres through prompts on videos, LIVEs and searches related to elections.</p> <p>From 18 Apr 2025 to 2 June 2025, we launched an in-app Election Centre to provide users with up-to-date information about the 2025 Portuguese election. The centre contained a section about spotting misinformation, which included videos created in partnership with our fact-checking partner Poligrafo.</p> <p>We directed people to the Election Centres through prompts on videos, LIVEs and searches related to elections.</p>
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available <p>The Election Centre, which launched in advance of the Portuguese election, was visited 371,857 times. This localised approach helped to ensure that messaging in relation to the election was relevant to our community and encouraged more engagement.</p>
Engagement with local and regional experts <i>(Commitment 17, Measure 17.2)</i>	Description of intervention <p>To further promote election integrity, and inform our approach to the Portuguese election, we organised an Election Speaker Series with Poligrafo who shared their insights and market expertise with our internal teams.</p>
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available <p>This engagement with external regional and local experts allowed us to inform our country-level approach to the election.</p>



Empowering the Research Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Providing access to our Research API <i>(Commitment 26 and Measures 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, and comments from our platform. More information is available here.</p>
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available <p>Number of Research API applications related to the Portuguese election that have been approved from January to June 2025: No applications received.</p>
Empowering the Fact-Checking Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Ensuring fact-checking coverage <i>(Commitment 30, Measure 30.1)</i>	Description of intervention <p>Poligrafo serves as the fact-checking partner for Portugal, which provided coverage for the platform.</p>
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available <p>Please see Chapter VII for relevant metrics.</p>



Reporting on the signatory's response during an election

2025 Romanian Presidential Election

Threats observed during the electoral period: [suggested character limit 2000 characters].

As co-chair of the Code of Conduct 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 Romanian Presidential Election, which took place on 4 May 2025, with a second round on 18 May 2025, following the unprecedented annulment of the 2024 results and marked one of the most closely monitored electoral cycles for TikTok to date.

From March to May 2025, TikTok deployed robust detection models, automated moderation, and local partnerships to safeguard its Romanian user base of over 8 million. The following are examples of some of the threats TikTok observed in relation to both election rounds:

- **Covert influence disruption:** TikTok reported removing two new domestic covert networks totaling 87 accounts and 33,296 followers in April 2025 for manipulating election discourse using fake news accounts and personas. More information relating to the network disruptions is published on our dedicated [Covert Influence Operations transparency page](#).
- **Content removals:** We removed over 13,100 pieces of election-related content in Romania for violating our policies on misinformation, civic integrity, and synthetic media - over 93% were taken down [before](#) any user report.
- We received 57 submissions through the COCD Rapid Response System in relation to the Romanian Presidential Election, which were rapidly addressed. Actions included banning or geo-blocking of accounts and content removals for violation of Community Guidelines.



Mitigations in place during the electoral period: [suggested character limit: 2000 characters].

A. Enforcing our policies

(I) Moderation capabilities

We supported the Romania 2025 elections by preparing moderators, updating policy, and escalating hate organization content in time for both election rounds. Our teams worked alongside technology to ensure that we consistently [enforced our rules](#) to detect and remove misinformation, covert influence operations, and other content and behaviour that can increase during an election period. We continue to prioritize and enhance TikTok's automated moderation technology as such technology enables faster and consistent removal of content that violates our rules. We invest in technologies that improve content understanding and predict potential risks so that we can take action on violative content before it's viewed.

We have thousands of trust and safety professionals dedicated to keeping our platform safe. We have 95 Romanian-speaking moderators, which is the largest such team among digital platforms in the country, both in absolute terms and relative to the number of users. We increased resources on our Romanian elections task force by adding more than 120 subject matter experts across multiple teams including Deceptive Behaviour (which includes Covert Influence Operations analysts), Security and Ads Integrity.

(II) Mission Control Centre: internal cross-functional collaboration

In advance of the official campaign period for the Romanian Presidential Election, we established a dedicated Mission Control Centre (MCC), including employees from multiple specialist teams within our safety department. Through the MCC, our teams were able to provide consistent and dedicated coverage of potential election-related issues in the run-up to, and during, the Romanian Presidential Election.

(III) Countering misinformation

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 are reflected in our approach. We also integrated the most recent insights from our expert partners into our policies and guidelines on misinformation and impersonation. We removed more than 5,500 pieces of election-related content in Romania for violating our policies on misinformation, harassment, and hate speech between March and May 2025.

(IV) Fact-checking

Our global fact-checking programme is a critical part of our layered approach to detecting harmful misinformation in the context of elections. The core objective of the fact-checking program is to leverage the expertise of external fact-checking organisations to help assess the accuracy of potentially harmful claims that are difficult to verify. TikTok collaborates with [12 fact-checking organizations](#) across Europe to evaluate the accuracy of content in most European languages, including Romanian. **LeadStories**, which is a verified member of International Fact-Checking Network and the European Fact-Checking Standards Network, serves as the fact-checking partner for Romania, which provided coverage for the platform, including across weekends.



(V) Deterring covert influence operations

We prohibit covert influence operations and remain constantly vigilant against attempts to use deceptive behaviours and manipulate our platform. We proactively seek and continuously investigate leads for potential influence operations. We're also working with government authorities and encourage them to share any intelligence so that we can work together to ensure election integrity. More detail on our policy against covert influence operations is published on our [website](#).

(VI) Tackling misleading AI-generated content

Creators are required to label any realistic AI-generated content (AIGC) and we have an [AI-generated content label](#) to help people do this. TikTok has a 'Edited Media and AI-Generated Content (AIGC)' policy, which prohibits AIGC showing fake authoritative sources or crisis events, or falsely showing public figures in certain contexts including being bullied, making an endorsement, or being endorsed.

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

We classify presidential candidate accounts as a Government, Politician, and Political Party Account ([GPPA](#)). We then apply designated policies to GPPAs to ensure the right experience, given their important role in civic processes. This includes disabling monetisation features.

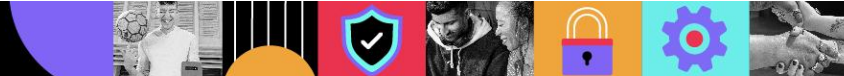
We strongly recommend that GPPAs be [verified](#). Verified badges help users make informed choices about the accounts they choose to follow. It is also an easy way for notable figures to let users know they're seeing authentic content, and it helps to build trust among high-profile accounts and their followers.

In advance of the elections TikTok's GR team organized dedicated sessions with every political group in Romania to inform about our policies and to educate political actors about safety measures. TikTok also requested a list of candidates be provided by the Romanian authorities to ensure the GPPA label could be correctly applied where relevant.

B. Directing people to trusted sources

(I) Investing in media literacy

We invest in media literacy campaigns as a counter-misinformation strategy. TikTok has partnered with the local NGO Funky Citizens in Romania to help the community safely navigate the platform and protect themselves against potential misinformation during the election. Funky Citizens developed a series of educational videos explaining how users could identify and avoid misinformation, use TikTok's safety features, and critically evaluate content related to the electoral process. The Romanian community could find the video series with practical advice and useful information about the electoral process on Funky Citizens' official TikTok account and the in-app Election Center dedicated to Romania's elections. These videos were viewed over 45 million times between March 2024 and February 2025.



C. External engagement at the national and EU levels

(I) Rapid Response System: external collaboration with COPD Signatories

The COPD Rapid Response System (RRS) was utilised to exchange information among civil society organisations, fact-checkers, and online platforms. TikTok received 57 notifications through the RRS in relation to the Romanian Election, which were addressed and actioned, enforcement included banning or geo-blocking of accounts and content removals for violation of Community Guidelines.

(II) Engagement with local experts

To further promote election integrity, and inform our approach to the Romanian Presidential Election, we organised an Election Speaker Series with Funky Citizens who shared their insights and market expertise with our internal teams.

(III) Engagement with national authorities pre-election

GR proactively organized an election-dedicated meeting on 7 February 2025 with ANCOM, the Permanent Electoral Authority and Ministry of Research, Innovation and Digitalization to establish points of contact before the elections and to offer access to our reporting tools including the Romanian election center. On 27 February 2025, we engaged in an online meeting with ANCOM and Autoritatea Electorală Permanentă, the Permanent Electoral Authority in Romania on new Romanian regulation .

On 3 March 2025, we participated in an ANCOM roundtable in Bucharest, as well as a series of meetings including an in-person tabletop exercise on the Romanian election.

In the run up to the 2025 election, and during the election period, we continued to engage with ANCOM and promptly responded to ongoing questions and correspondence

[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 (Integrity and Authenticity) Policies	N/A		
Scrutiny of Ads Placements			
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.			
Scrutiny of Ad Placements, including prohibition on monetisation and fundraising campaigns for GPPAs (Commitment 1 and Measure 1.1)	Description of intervention		
	TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document .		
Scrutiny of Ad Placements, including prohibition on monetisation and fundraising campaigns for GPPAs (Commitment 1 and Measure 1.1)	Indication of impact (at beginning of action: expected impact) including relevant metrics when available		
	N/A		
Political Advertising			



Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Prohibition on Political Advertising <i>(Commitment 5, Measure 5.1)</i>	Description of intervention TikTok did not subscribe to this commitment as outlined in the January 2025 Subscription Document .
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available N/A
Integrity of Services	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Identifying and removing CIO networks <i>(Commitment 14, Measure 14.1)</i>	Description of intervention During the Romanian Presidential Election, we continued our work to detect and disrupt covert influence operations (CIOs) that attempt to establish themselves on TikTok and undermine the integrity of our platform.
	Indication of impact (at beginning of action: expected impact) including relevant metrics when available TikTok has scaled mitigations against deceptive behaviours including spam, impersonation, and activities in relation to fake engagement. As examples of our efforts in this area, from March to May 2025: <ul style="list-style-type: none"> • We proactively prevented more than 21.5 million fake likes and 8.09+ million fake follow requests, and we blocked 38,000 spam accounts from being created in Romania. We also removed: <ul style="list-style-type: none"> ○ 48,300 fake accounts ○ 8.2+ million fake likes ○ 1.83+ million fake followers • From 1 September 2024 to 26 May 2025, we prevented more than 120 million fake likes and more than 53 million fake follow requests, and we blocked more than 707,670 spam accounts from being created in Romania. We also removed: over 2,000 accounts impersonating Romanian Government, Politician, or Political Party Accounts, 379,324 fake accounts, 28.9+ million fake likes and 15.6+ million fake followers.



	<p>As set out above we reported removing two CIO networks in 2025 that were identified as specifically targeting a Romanian audience, including:</p> <ul style="list-style-type: none"> • A network of 27 accounts that had 9,474 cumulative followers as at the date of removal, operating from Romania that attempted to target Romanian audiences in order to amplify certain narratives, attempting to manipulate Romanian elections discourse. The network was found to create accounts with generic handles and avatars which it presented as news accounts. • A network of 60 accounts that had 23,822 cumulative followers as at the date of removal, operating from Romania that attempted to target Romanian audiences in order to amplify certain narratives, attempting to manipulate Romanian elections discourse. The network was found to create fictitious personas in order to post comments and content aligned with its strategic goal. <p>More information relating to the above detailed network disruptions is published on our dedicated Covert Influence Operations transparency page.</p>
<p>Tackling misleading AIGC and edited media</p> <p><i>(Commitment 15, Measures 15.1 and 15.2)</i></p>	<p style="text-align: center;">Description of intervention</p> <p>Our Edited Media and AI-Generated Content (AIGC) policy makes it clear that we do not want our users to be misled about political issues. For the purposes of our policy, AIGC refers to content created or modified by artificial intelligence (AI) technology or machine-learning processes, which may include images of real people, and may show highly realistic-appearing scenes, or use a particular artistic style, such as a painting, cartoons, or anime.</p> <p>We do not allow misleading AIGC or edited media that falsely shows:</p> <ul style="list-style-type: none"> • Content made to seem as if it comes from an authoritative source, such as a reputable news organisation, • A crisis event, such as a conflict or natural disaster, • A public figure who is: <ul style="list-style-type: none"> ○ being degraded or harassed, or engaging in criminal or anti-social behaviour ○ taking a position on a political issue, commercial product, or a matter of public importance (such as an election) ○ being politically endorsed or condemned by an individual or group. <p>In addition, all AIGC or edited media, including that which depicts public figures, such as politicians, must be clearly labelled as AI generated, and can not be used for endorsements.</p> <p>As AI evolves, we continue to invest in combating harmful AIGC by evolving our proactive detection models, consulting with experts, and partnering with peers on shared solutions.</p>



	<p>TikTok has invested in labeling technologies and tools, including the implementation of Content Credentials technology from the Coalition for Content Provenance and Authenticity (C2PA), which enables the automatic recognition and labeling of AI-generated content. This is complemented by a TikTok-developed tool that allows creators to easily label AI-generated content, already used by 37 million creators. TikTok's commitment to AIGC transparency ensures a safe environment for users, who can easily identify synthetic content and understand its context.</p> <p>TikTok is a member of the Content Authenticity Initiative and the Coalition for Content Provenance and Authenticity, and was the first video sharing platform to put Content Credentials into practice. We have the ability to read Content Credentials that attach metadata to content, which we can use to instantly recognise and label AIGC. This helped us to expand auto-labelling to AIGC created on some other platforms.</p> <p>These measures are supported by strategic collaborations with other leading tech companies to combat AI-generated misinformation. Furthermore, TikTok supports the new guidelines of the International Foundation for Electoral Systems.</p> <p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>Number of videos removed because of violation of Edited Media and AI-Generated Content (AIGC) from 31 March to 6 April 2025 and 12-18 May 2025 to cover both rounds of elections and the 4 weeks leading up to Round 1 of the Romanian Presidential Election: 657</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 (Commitment 17, Measure 17.2)</p>	<p>Description of intervention</p> <p>TikTok had an in-app Election Center dedicated to Romania's Presidential election. We updated our in-app Election Center to directly link to the Electoral Commission's website so it's even easier for people to access authoritative election information. In line with media literacy best practices, we also added a reminder to verify the accuracy of election information people see online and off.</p> <p>TikTok also partnered with local NGO Funky Citizens to help the community safely navigate the platform and protect themselves against potential misinformation during the election. The Center featured authoritative information from Funky Citizens, Libertatea, and Digi FM, and was promoted to users through search guides and automatic content labels.</p>



	Funky Citizens developed a series of educational videos explaining how users could identify and avoid misinformation, use TikTok's safety features, and critically evaluate content related to the electoral process. The Romanian community could find the video series with practical advice and useful information about the electoral process on Funky Citizens' official TikTok account and in the Election Center.
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>The in-app Election Center launched before the Presidential Election was visited 2,018,869 times between 31 March and 23 May.</p> <p>Funky Citizens videos were viewed over 45 million times between March 2024 and February 2025.</p>
Engagement with local and regional experts (<i>Commitment 17, Measure 17.2</i>)	<p>Description of intervention</p> <p>To further promote civic awareness, TikTok introduced a permanent media literacy hub on 14 May 2025, surfacing critical thinking tools via keyword-triggered notices. Additionally, Romanian influencers and marketing agencies were briefed on TikTok's strict rules against political advertising and branded content.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>This engagement with external regional and local experts allowed TikTok to inform its approach to the Romanian Presidential Election.</p>
<p>Empowering the Research Community</p>	
<p>Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.</p>	
Providing access to our Research API <i>(Commitment 26 and Measures 26.1 and 26.2)</i>	<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, and comments from our platform. More information is available here.</p>



	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>Number of Research API applications related to the Romanian Presidential Election received January to June 2025: 7</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>Ensuring fact-checking coverage (Commitment 30, Measure 30.1)</p>	<p>Description of intervention</p> <p>LeadStories serves as the fact-checking partner for Romania, which provided coverage for the platform, including across weekends in advance of the Romanian Presidential Election.</p>
	<p>Indication of impact (at beginning of action: expected impact) including relevant metrics when available</p> <p>In May 2025, LeadStories provided 77 misinformation leads and submitted an Insights Report focused on the Romanian election. Please refer to Chapter 7 - Empowering the Fact-Checking Community for comprehensive metrics.</p>