

Code of Practice on
Disinformation – Report of
TikTok for the period 1
January 2023 - 30 June
2023

Table of Content

II. Scrutiny of Ad Placements	1
Commitment 1	1
Commitment 2	8
Commitment 3	12
III. Political Advertising	14
Commitment 4	15
Commitment 5	15
Commitment 6	16
Commitment 7	19
Commitment 8	21
Commitment 9	22
Commitment 10	22
Commitment 11	23
Commitment 12	24
Commitment 13	25
IV. Integrity of Services	26
Commitment 14	27
Commitment 15	42
Commitment 16	43
V. Empowering Users	44
Commitment 17	45
Commitment 18	48
Commitment 19	49
Commitment 20	50
Commitment 21	51
Commitment 22	54
Commitment 23	59
Commitment 24	59
Commitment 25	60
VI. Empowering the research community	62
Commitment 26	63
Commitment 27	64
Commitment 28	65
Commitment 29	66
VII. Empowering the fact-checking community	68
Commitment 30	69
Commitment 31	71
Commitment 32	76
Commitment 33	77

VIII. Transparency Centre	78
Commitment 34	79
Commitment 35	80
Commitment 36	81
IX. Permanent Task-Force	82
Commitment 37	83
X. Monitoring of Code	84
Commitment 38	85
Commitment 39	85
Commitment 40	86
Commitment 41	87
Commitment 42	88
Commitment 43	88
Commitment 44	89
Reporting on the service's response during a period of crisis	90
Covid-19 pandemic	91
War of aggression by Russia on Ukraine	93

Commitments	Measures	Service A
II. Scrutiny of Ad Placements		
1	Measure 1.1	☒
	Measure 1.2	☒
	Measure 1.3	☒
	Measure 1.4	☒
	Measure 1.5	☒
	Measure 1.6	☒
2	Measure 2.1	☒
	Measure 2.2	☒
	Measure 2.3	☒
	Measure 2.4	☒
3	Measure 3.1	☒
	Measure 3.2	☒
	Measure 3.3	☒
III. Political advertising		
4	Measure 4.1	☒

	Measure 4.2	<input checked="" type="checkbox"/>
5	Measure 5.1	<input checked="" type="checkbox"/>
6	Measure 6.1	<input checked="" type="checkbox"/>
	Measure 6.2	<input checked="" type="checkbox"/>
	Measure 6.3	<input checked="" type="checkbox"/>
	Measure 6.4	<input checked="" type="checkbox"/>
	Measure 6.5	<input type="checkbox"/>
7	Measure 7.1	<input checked="" type="checkbox"/>
	Measure 7.2	<input checked="" type="checkbox"/>
	Measure 7.3	<input checked="" type="checkbox"/>
	Measure 7.4	<input checked="" type="checkbox"/>
8	Measure 8.1	<input checked="" type="checkbox"/>
	Measure 8.2	<input checked="" type="checkbox"/>
9	Measure 9.1	<input checked="" type="checkbox"/>
	Measure 9.2	<input checked="" type="checkbox"/>
10	Measure 10.1	<input checked="" type="checkbox"/>
	Measure 10.2	<input checked="" type="checkbox"/>

11	Measure 11.1	<input checked="" type="checkbox"/>
	Measure 11.2	<input checked="" type="checkbox"/>
	Measure 11.3	<input checked="" type="checkbox"/>
	Measure 11.4	<input checked="" type="checkbox"/>
12	Measure 12.1	<input type="checkbox"/>
	Measure 12.2	<input type="checkbox"/>
	Measure 12.3	<input type="checkbox"/>
13	Measure 13.1	<input checked="" type="checkbox"/>
	Measure 13.2	<input checked="" type="checkbox"/>
	Measure 13.3	<input checked="" type="checkbox"/>
IV. Integrity of services		
14	Measure 14.1	<input checked="" type="checkbox"/>
	Measure 14.2	<input checked="" type="checkbox"/>
	Measure 14.3	<input checked="" type="checkbox"/>
15	Measure 15.1	<input checked="" type="checkbox"/>
	Measure 15.2	<input checked="" type="checkbox"/>
16	Measure 16.1	<input checked="" type="checkbox"/>
	Measure 16.2	<input checked="" type="checkbox"/>

V. Empowering users

17	Measure 17.1	<input checked="" type="checkbox"/>
	Measure 17.2	<input checked="" type="checkbox"/>
	Measure 17.3	<input checked="" type="checkbox"/>
18	Measure 18.1	<input checked="" type="checkbox"/>
	Measure 18.2	<input checked="" type="checkbox"/>
	Measure 18.3	<input checked="" type="checkbox"/>
19	Measure 19.1	<input checked="" type="checkbox"/>
	Measure 19.2	<input checked="" type="checkbox"/>
20	Measure 20.1	<input type="checkbox"/>
	Measure 20.2	<input type="checkbox"/>
21	Measure 21.1	<input checked="" type="checkbox"/>
	Measure 21.2	<input checked="" type="checkbox"/>
	Measure 21.3	<input checked="" type="checkbox"/>
22	Measure 22.1	<input type="checkbox"/>
	Measure 22.2	<input type="checkbox"/>
	Measure 22.3	<input type="checkbox"/>

	Measure 22.4	<input type="checkbox"/>
	Measure 22.5	<input type="checkbox"/>
	Measure 22.6	<input type="checkbox"/>
	Measure 22.7	<input checked="" type="checkbox"/>
23	Measure 23.1	<input checked="" type="checkbox"/>
	Measure 23.2	<input checked="" type="checkbox"/>
24	Measure 24.1	<input checked="" type="checkbox"/>
25	Measure 25.1	<input type="checkbox"/>
	Measure 25.2	<input type="checkbox"/>
VI. Empowering the research community		
26	Measure 26.1	<input checked="" type="checkbox"/>
	Measure 26.2	<input checked="" type="checkbox"/>
	Measure 26.3	<input checked="" type="checkbox"/>
27	Measure 27.1	<input checked="" type="checkbox"/>
	Measure 27.2	<input checked="" type="checkbox"/>
	Measure 27.3	<input checked="" type="checkbox"/>
	Measure 27.4	<input checked="" type="checkbox"/>
28	Measure 28.1	<input checked="" type="checkbox"/>

	Measure 28.2	<input checked="" type="checkbox"/>
	Measure 28.3	<input checked="" type="checkbox"/>
	Measure 28.4	<input checked="" type="checkbox"/>
29	Measure 29.1	<input type="checkbox"/>
	Measure 29.2	<input type="checkbox"/>
	Measure 29.3	<input type="checkbox"/>
VII. Empowering the fact-checking community		
30	Measure 30.1	<input checked="" type="checkbox"/>
	Measure 30.2	<input checked="" type="checkbox"/>
	Measure 30.3	<input checked="" type="checkbox"/>
	Measure 30.4	<input checked="" type="checkbox"/>
31	Measure 31.1	<input checked="" type="checkbox"/>
	Measure 31.2	<input checked="" type="checkbox"/>
	Measure 31.3	<input checked="" type="checkbox"/>
	Measure 31.4	<input checked="" type="checkbox"/>
32	Measure 32.1	<input checked="" type="checkbox"/>
	Measure 32.2	<input checked="" type="checkbox"/>
	Measure 32.3	<input checked="" type="checkbox"/>

33	Measure 33.1	<input type="checkbox"/>
VIII. Transparency centre		
34	Measure 34.1	<input checked="" type="checkbox"/>
	Measure 34.2	<input checked="" type="checkbox"/>
	Measure 34.3	<input checked="" type="checkbox"/>
	Measure 34.4	<input checked="" type="checkbox"/>
	Measure 34.5	<input checked="" type="checkbox"/>
35	Measure 35.1	<input checked="" type="checkbox"/>
	Measure 35.2	<input checked="" type="checkbox"/>
	Measure 35.3	<input checked="" type="checkbox"/>
	Measure 35.4	<input checked="" type="checkbox"/>
	Measure 35.5	<input checked="" type="checkbox"/>
	Measure 35.6	<input checked="" type="checkbox"/>
36	Measure 36.1	<input checked="" type="checkbox"/>
	Measure 36.2	<input checked="" type="checkbox"/>
	Measure 36.3	<input checked="" type="checkbox"/>
IX. Permanent Task-Force		

37	Measure 37.1	☒
	Measure 37.2	☒
	Measure 37.3	☒
	Measure 37.4	☒
	Measure 37.5	☒
	Measure 37.6	☒
X. Monitoring of the Code		
38	-	☒
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	<input checked="" type="checkbox"/>
42	-	<input checked="" type="checkbox"/>
43	-	<input checked="" type="checkbox"/>
44	-	<input checked="" type="checkbox"/>

About TikTok

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

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

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

Our second report under the Code - 1 January to 30 June 2023

Since 2020, TikTok has been committed to, and heavily involved, in the Code process. We continue to meaningfully engage in the Code's Taskforce and all of its working groups and subgroups. TikTok is co-chair of the working group on Elections and has taken a leading role in supporting TrustLab's Structural Indicators pilot.

The positive reception TikTok received to its baseline report underlines the significant resources and time we have committed across many teams to the Code. We set a high bar in our first report as we provided detailed descriptions of the measures we take and disclosed robust, granular data in support of those measures. For our second report, we are pleased to confirm that we have continued to build on our existing measures over the last six months, including rapidly scaling up our fact-checking programme to provide coverage in an additional 9 countries, and advancing our rules on synthetic media. We have also increased the number of data points disclosed to over 2,600 data points by innovating to produce new metrics, enabling us to further enhance transparency for our community.

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

Our policies

In the spirit of continuous improvement, we are always reviewing and developing our policies. We recently carried out our most comprehensive [update](#) to our Community Guidelines (**CGs**) to date by offering our community enhanced transparency about our rules and how we enforce them. The updates provide more information around key policy areas such as how we protect [civic and election integrity](#) and treat content containing [synthetic media](#).

Our Integrity and Authenticity policies aim to promote a trustworthy, authentic experience for our users. Our policies focus on harmful misinformation (rather than making a distinction between disinformation and misinformation) and deceptive behaviours.¹ We do not allow inaccurate, misleading, or false content that may cause significant harm to individuals or society, regardless of

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

intent. These policies can be applied to a wide range of content, and that's by design; this content is constantly changing, often based on what's happening in the world. We also tackle deceptive behaviour by removing accounts that seek to mislead people or attempt to use TikTok to deceptively sway public opinion.

Enforcing our policies

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

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

By rapidly expanding our fact-checking programme to nine new EU countries over the past six months, and together with expanding our specialised misinformation moderation teams and strengthening our machine learning models, our numbers show our increased ability to remove more complex harmful misinformation.

Demonetisation

TikTok has been operating for a much shorter length of time than other platforms and therefore, creator monetisation opportunities are at a relatively early stage of maturity. We are fully committed to rewarding creativity and equipping creators with the best tools to find their community, grow their careers and unlock exciting opportunities both on and off the platform.

Like all users of our platform, participants in content monetisation programs must adhere to our CGs, 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.

Transparency of Advertising

Ads must comply with our strict policies and all ads are reviewed against these policies before being allowed on our platform. Our ad policies specifically prohibit misleading, inauthentic and deceptive behaviours. We are continually improving our policies and have developed four more granular harmful misinformation ad policies, covering medical misinformation, dangerous misinformation, manipulated media and dangerous conspiracy theories.

We do not allow [political actors](#) to place ads, nor do we allow anyone to place [political ads](#). We do allow cause based advertising and public services advertising from government agencies, non-profits and other entities if they are not driven by partisan political motives.

We are pleased to confirm that we have further increased transparency about ads on our platforms by disclosing new metrics in this report including the number of views of violative ads.

We continue to engage with external stakeholders and have increased our alignment with IAB Sweden and Ireland, achieving Gold Standard certification in these countries. As a Global Alliance for

Responsible Median (GARM) member, we also remain committed to upholding the GARM Framework and, as part of that, removing harmful misinformation from monetisation.

Ensuring the Integrity of Services

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

As part of our [CGs refresh](#), we launched our updated synthetic media policy to address the use of content created or modified by AI technology on our platform. 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. Synthetic media that is not disclosed or is otherwise in violation of our policy is prohibited on our platform.

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

Empowering Users

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

Together with systematically removing content from our platform that violates our policies, we have dedicated significant resources to increasing the number of in-app measures that show users additional context on certain content, redirect them to authoritative information and encourage them to report any potential misinformation on the topic. We keep under review what topics to develop interventions for and recently, we rolled out a search intervention on [climate change](#). We make these tools available in 23 official languages.

We continue to be involved in a variety of on and off-platform media literacy campaigns in close collaboration with our fact-checking partners. We rolled-out eight localised campaigns addressing disinformation related to the war in Ukraine as well as election integrity campaigns in advance of the Spanish, Greek and Finnish elections. We will be running similar campaigns in the run up to the Polish and Slovakian elections. We have not been able to produce certain metrics for our most recent election campaigns and we are working hard to address this for future reports.

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 that their For You feed is based on a personalised recommendation system and have refreshed the information we provide users about the way in which our [recommender systems](#) operate.

To provide users with more choice about their recommender systems, we have introduced a feature that enables users to [refresh their For You feed](#). We are also providing our European community with more ways to discover content on TikTok [by allowing them to turn off personalisation](#). This means their For You and LIVE feeds will instead show popular videos from both the places where they live and around the world, rather than recommending content to them based on their personal interests.

Our report describes how we build safety into our recommendations. As well as removing harmful misinformation content that violates our CGs, we take steps to avoid recommending certain categories of content that may not be appropriate for a general audience. We have made even clearer to our users [here](#) that certain content is ineligible for the For You feed, including general conspiracy theories, unverified information relating to an emergency or unfolding event and potential high-harm misinformation undergoing fact checking assessment. Since August 2023, we have been notifying

creators when their content has been made ineligible for recommendation and enabling them to [appeal](#).

Empowering Researchers

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

We have been publishing our [CG Enforcement Reports](#) since 2020 in order to bring transparency around how we operate and protect our platform. More recently, we have expanded our [Research API](#) (which provides researchers with access to public data on content and accounts from our platform) to Europe and rolled-out a number of [improvements](#). We have also introduced our [Commercial Content API](#) to bring transparency to paid advertising and other content that's commercial in nature on TikTok. The development of these tools was informed by feedback we have heard from researchers and civil society.

We are participating in a data access pilot with EDMO in order to trial the process for sharing data with vetted researchers as designated under the DSA.

Empowering the Fact-Checking Community

TikTok recognises the important contribution of fact-checkers to the fight against disinformation. We are proud to have sponsored and presented at the annual [GlobalFact10](#) summit, which was hosted by the [IFCN](#).

TikTok's fact-checking programme differs from that of other platforms, as we incorporate fact-checker input into our broader content moderation efforts. This means that this feedback is relayed to TikTok's moderation teams so that they can ensure it is factored into their moderation work. This approach effectively produces a force multiplier to the underlying fact-checking output, ensuring that the disinformation content or trend is more comprehensively and broadly addressed.

We have continued to progress the rapid scale-up of our fact-checking program across Europe and we have launched fact-checking programs in nine new EU countries, meaning that we now have coverage in 17 official EU languages and the spoken language of 23 EEA countries. As we built momentum with our fact-checking partners, the metrics reflect our increased ability to identify and remove more complex harmful misinformation.

We also revamped our agreements with our fact-checking partners in order to reflect feedback from our partners and build in further flexibility to facilitate our partners debunking an expanded type of claims in further languages and supporting additional ad hoc projects. We have increased our ability to receive proactive flagging of potential misinformation from our fact-checking partners and implemented a pilot scheme to share enforcement data with our fact-checking partners on the claims they have provided feedback on.

Looking forward

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

We are committed to continuing to develop and enhance our policies and tools ahead of the next Code report in 2024.

II. Scrutiny of Ad Placements Commitments 1 - 3

II. Scrutiny of Ad Placements

Commitment 1

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

<p>In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]</p>	<p>Yes</p>
<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> ● In order to improve our existing ad policies, developed four more granular policies and as a result also expanded our existing policy coverage, and aligned them with our existing CGs. These four policies are: <ul style="list-style-type: none"> ○ Medical Misinformation ○ Dangerous Misinformation ○ Manipulated Media ○ Dangerous Conspiracy Theories ● Expanded our operational coverage in the EEA of our in-house pre-campaign brand safety tool, the TikTok Inventory Filter. ● Increased transparency around harmful misinformation and ads and have disclosed a number of additional metrics for this Chapter of the report. ● Continued to regularly participate in the working group on Ad Scrutiny.
<p>Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]</p>	<p>Yes</p>

<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> • Continuing the implementation and enforcement of our four more granular and improved harmful misinformation ad policies. • Developing and implementing further policies targeted at specific types of harmful misinformation to increase the granularity of our ad policies. • Looking into increasing the implementation of our third party post-campaign brand safety solutions provided by Integral Ad Science (IAS) and DoubleVerify across the EEA. • Continuing our expansion of the TikTok Inventory Filter within the EEA.
<p>Measure 1.1</p>	
<p>QRE 1.1.1</p>	<p>To help keep our platform welcoming and authentic for everyone, we take seriously ensuring it is free from harmful misinformation.</p> <p>(I) Our policies and approach</p> <p>Our I&A policies within our CGs are the first line of defence in combating harmful misinformation and deceptive behaviours on our platform. All users are required to comply with these CGs. Where content on our platform is deemed violative of our CGs, we remove it.</p> <p>Paid ads are also subject to our strict ad policies and are reviewed against these policies before being allowed on our platform. Our ad policies specifically prohibit misleading, inauthentic and deceptive behaviours. Ads deemed in violation of these policies will not be permitted on our platform, and accounts deemed in severe or repeated violation may be suspended or banned.</p> <p>We are pleased to confirm that in order to improve our existing ad policies, we have developed four more granular policies and as a result also expanded our existing policy coverage. These four are:</p> <ul style="list-style-type: none"> • Medical Misinformation • Dangerous Misinformation • Manipulated Media • Dangerous Conspiracy Theories <p>We are progressing with fully implementing these policies and reflecting on whether there are further focused areas we should consider developing policies for.</p>

We also have specific ad policies that focus on certain topics where the risk of disinformation may be higher.

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

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

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

(II) Verification in the context of ads

Our [strict ad policies](#) require advertisers to meet a number of requirements regarding the landing page. For example, the landing page must be functioning and must contain complete and accurate information including about the advertiser. Ads risk not being approved if the product or service advertised on the landing page does not match that included in the ad.

We also provide verified badges on some accounts including certain advertisers. Verified badges help users make informed choices about the accounts they choose to follow. It's an easy way for notable figures to let users know they're seeing authentic content, and it helps to build trust among high-profile accounts and their followers. For individuals, non-profits, institutions, businesses, or official brand pages, this badge builds an important layer of clarity with the TikTok community. We consider a number of factors before granting a verified badge, such as whether the notable account is authentic, unique, and active.

² See the 'Political and Issue Based Advertising' section

	<p>We are currently trialling mandatory verification for accounts belonging to a government, politician, or political party in the US. Meanwhile, in the EU, verification is available for these types of accounts. We also apply a number of policies that help prevent misuse of certain features e.g., access to advertising features and solicitation for campaign fundraising are not allowed.</p>			
<p>SLI 1.1.1 – Numbers by actions enforcing policies above (specify if at page and/or domain level)</p>	<p>Methodology of data measurement:</p> <p>We have set out the number of ads that have been removed from our platform for violation of our Covid-19 misinformation and political content policies respectively. Note that numbers have only been provided for monetised markets and are based on where the ads were displayed.</p> <p>As mentioned above, in order to improve our existing ad policies, we have recently developed four more granular policies and as a result also expanded our existing policy coverage. As these policies were launched towards the end of the reporting period, we do not have meaningful data to share for this report, but we expect to be able to provide this data in the next report.</p> <p>We are pleased to be able to include the impressions data for ads removed for the below policies in this report.</p>			
	<p>Number of ad removals under the Covid-19 misinformation ad policy</p>	<p>Number of ad removals under the political content ad policy</p>		
<p>Member States</p>				
<p>Austria</p>	<p>1</p>	<p>16</p>		
<p>Belgium</p>	<p>10</p>	<p>10</p>		
<p>Bulgaria</p>	<p>0</p>	<p>0</p>		

Croatia	0	0		
Cyprus	0	0		
Czech Republic	1	10		
Denmark	0	3		
Estonia	0	0		
Finland	0	8		
France	1	41		
Germany	1	33		
Greece	0	0		
Hungary	0	12		
Ireland	2	23		
Italy	3	47		

Latvia	0	0		
Lithuania	0	0		
Luxembourg	0	0		
Malta	0	0		
Netherlands	0	48		
Poland	1	49		
Portugal	0	3		
Romania	0	14		
Slovakia	0	0		
Slovenia	0	0		
Spain	0	68		
Sweden	0	5		

Iceland	0	0		
Liechtenstein	0	0		
Norway	0	5		
Total EU	20	390		
Total EEA	20	395		

This additional Service Level Indicator provides an estimated financial value of the actions taken by Signatories to demonetise disinformation sources (under SLI 1.1.1). It is based on media metrics available to Signatories (query/bid³ or impression⁴) and applying an agreed-upon conversion factor provided by a third party designated by the Task-force of the Code (Ebiquity plc.).

SLI 1.1.2 - Preventing the flow of legitimate advertising investment to sites or content that are designated as disinformation	We were pleased to be able to report impressions for ads removed for the first time in this report. We continue to be committed to increasing transparency in this chapter and participating in the working group.
Member States	Euro value of ads demonetised
Total EU	N/A

³ Request placed between a seller and buyer of advertising that can detail amongst other things website, specific content, targeting data inclusive of audience or content.

⁴ Comprehensive calculation of the number of people who have been reached by a piece of media content by passive exposure (viewing a piece of content) or active engagement (visiting a destination).

Total EEA	N/A
------------------	-----

Measure 1.2				
QRE 1.2.1	<p>We do not currently offer ad revenue sharing in the EEA.</p> <p>We offer creator monetisation opportunities such as the TikTok Creator Fund/ Creativity Program Beta. These programs offer creators meeting certain eligibility criteria the opportunity to join in order to monetise their content based on the level of user interaction with the videos they post.</p> <p>All creators must comply with TikTok’s CGs, including our I&A policies. Where creators fail to comply with our CGs, this may result in loss of access to monetisation and / or loss of account access. Users in all EU member states are notified by an in-app notification in their relevant local language where there has been a restriction of their ability to monetise, restriction of their access to a feature, removal or otherwise restriction of access to their content, or a ban of their account.</p> <p>We prohibit accounts verified as belonging to a government, politician or political party from accessing monetisation features. Specifically, they will not have access to features like ‘tips’, or the possibility of collecting ‘diamonds’, and will be ineligible for participation in other content monetisation programs like our Creator Fund. These changes, along with our existing ban on political advertising, mean that accounts belonging to politicians, political parties and governments will not be able to give or receive money through TikTok’s monetisation features, or spend money promoting their content (although exemptions are made for governments in certain circumstances e.g., for public health).</p>			
SLI 1.2.1	<p>Methodology of data measurement:</p> <p>We are unable to report on this data at present and are working towards being able to.</p>			
Member States	N/A	N/A	N/A	N/A
Total EU				
Total EEA				

Measure 1.3	
QRE 1.3.1	<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. These measures are in addition to the CGs and will apply to any content that appears in the For You feed (since this can comprise both ads and other types of content):</p> <ul style="list-style-type: none"> ● TikTok Inventory Filter: This is our proprietary system which enables advertisers to choose the content they want their ads to run adjacent to. The Inventory Filter is embedded directly in TikTok Ads Manager, the system through which advertisers purchase ads, and informed by the GARM Framework. More details can be found here. The Inventory Filter policies include topics which may be susceptible to disinformation. ● TikTok Brand Safety by Integral Ad Science (“IAS”): Advertisers can select IAS within the platform to ensure their ads run near content verified by IAS. IAS verifies content against the GARM Framework. Some disinformation content may be filtered by IAS as a result of the existing GARM Framework categories, such as Sensitive Social Issues. <p>Transparency: We have partnered with third parties to offer post-campaign solutions that enable advertisers to assess the suitability of user content that ran immediately adjacent to their ad in the For You feed:</p> <ul style="list-style-type: none"> ● Zefr: Through our partnership with Zefr, advertisers can obtain campaign insights into brand suitability and safety on the platform. Zefr is fully aligned with the GARM Framework. ● IAS: Advertisers can measure brand safety, viewability and invalid traffic on the platform with the IAS Signal platform. As with IAS’s pre-bid solution covered above, IAS is aligned with the GARM Framework. ● DoubleVerify: We are partnering with DoubleVerify to provide advertisers with media quality measurement for ads. DoubleVerify is working actively with us to expand their suite of brand suitability and media quality solutions on the platform.

Measure 1.4	
QRE 1.4.1	<p>When TikTok advertises, we buy advertising space only through ad networks (either directly or through agencies) which make available to us robust and reputable brand safety tools, which mitigate the risk of TikTok ads appearing next to sources of disinformation.</p> <p>As well as making IAS available on the platform, we make use of IAS to ensure our own ads run on or near suitable content. Using GARM standards, IAS reports on content which has been filtered or flagged and allows us to make changes to the context filters to avoid ads appearing next to similar content in the future by activating pre- and post-impression blocks towards unsafe content, themes and keywords.</p> <p>We monitor the placement of our ads closely (especially in the context of politically sensitive events including the Ukraine War) and in the event our ads are found to run adjacent to or on sources of disinformation, we will investigate to determine whether the content in question has been correctly identified and verify this with IAS or GARM as appropriate. We will then adjust any filters or add the publication in question to a blocklist to prevent a recurrence.</p> <p>When purchasing advertising space through ad networks, we make use of IAS in the way set out above, in addition to various brand safety tools to prevent TikTok ads appearing next to sources of disinformation.</p>
Measure 1.5	
QRE 1.5.1	<p>We have achieved the TAG Brand Safety Certified seal and the TAG Certified Against Fraud seal by the Trustworthy Accountability Group (“TAG”) in the EEA and globally. We provided access to external auditors who verified us for these. Details of our TAG seal can be found by searching for “TikTok” on their public register which can be found here.</p> <p>We have been certified by the Interactive Advertising Bureau (“IAB”) for the IAB Ireland Gold Standard 2.1 (listed here) and IAB Sweden Gold Standard 1.0 (listed here).</p>
QRE 1.5.2	<p>We have achieved the TAG Brand Safety Certified and TAG Certified Against Fraud Seals and the IAB Ireland Gold Standard and IAB Sweden Gold Standard 1.0.</p>

Measure 1.6	
QRE 1.6.1	<p>We offer a variety of brand safety tools for preventing ads from being placed beside specific types of content. We partner with third parties such as IAS.</p> <p>We are also exploring what other partnerships, including with researchers, may be appropriate for our platform. Furthermore, our strict advertising policies help to ensure that the categories of content which are most likely to require such checks and integration of information do not make it onto the platform in the first place.</p>
QRE 1.6.2	We only purchase ads through ad networks which make available to us robust and reputable brand safety tools. All of our media investment is thus protected by such tools
QRE 1.6.3	We have partnered with several third parties (IAS, Double Verify and Zefr) to offer post-campaign solutions that enable advertisers to assess the suitability of user content that ran immediately adjacent to their ad in the For You feed.
QRE 1.6.4	Not applicable as TikTok does not rate sources.
SLI 1.6.1	N/A
	N/A
Data	N/A

II. Scrutiny of Ad Placements

Commitment 2

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

<p>In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]</p>	<p>Yes</p>
<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> ● In order to improve our existing ad policies, developed four more granular policies and as a result also expanded our existing policy coverage. These four policies are: <ul style="list-style-type: none"> ○ Medical Misinformation ○ Dangerous Misinformation ○ Manipulated Media ○ Dangerous Conspiracy Theories
<p>Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> ● Developing and implementing further ad policies targeted at specific types of harmful misinformation. ● Continuing the implementation and enforcement of our four more granular, expanded and improved harmful misinformation ad policies.

Measure 2.1			
QRE 2.1.1	Paid ads are subject to our strict ad policies , which specifically prohibit misleading, inauthentic and deceptive behaviours. All ads are reviewed against these policies before being allowed on our platform. In order to improve our existing ad policies, we have recently developed four more granular policies (namely, Medical Misinformation, Dangerous Misinformation, Manipulated Media and Dangerous Conspiracy Theories) which advertisers also need to comply with.		
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 Covid-19 misinformation, and political content respectively. Note that numbers have only been provided for monetised markets and are based on where the ads were displayed.</p> <p>As mentioned above, in order to improve our existing ad policies, we have recently developed four more granular policies and as a result also expanded our existing policy coverage. As these policies were launched towards the end of the reporting period, we do not have meaningful data to share for this report, but we expect to be able to provide this data in the next report.</p>		
	Number of ad removals under the Covid-19 misinformation ad policy	Number of ad removals under the political content ad policy	
Member States			
Austria	1	16	
Belgium	10	10	
Bulgaria	0	0	
Croatia	0	0	

Cyprus	0	0		
Czech Republic	1	10		
Denmark	0	3		
Estonia	0	0		
Finland	0	8		
France	1	41		
Germany	1	33		
Greece	0	0		
Hungary	0	12		
Ireland	2	23		
Italy	3	47		
Latvia	0	0		
Lithuania	0	0		
Luxembourg	0	0		
Malta	0	0		
Netherlands	0	48		
Poland	1	49		
Portugal	0	3		
Romania	0	14		
Slovakia	0	0		

Slovenia	0	0		
Spain	0	68		
Sweden	0	5		
Iceland	0	0		
Liechtenstein	0	0		
Norway	0	5		
Total EU	20	390		
Total EEA	20	395		

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

	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.			
SLI 2.3.1	We are pleased to be able to report on the ads removed for breach of our Covid-19 misinformation and political content policies, including the impressions of those ads in this report.			
	Number of ad removals under the Covid-19 misinformation ad policy	Number of ad removals under the political content ad policy	Number of impressions for ads removed under the Covid-19 misinformation ad policy	Number of impressions for ads removed under the political content ad policy
Member States				
Austria	1	16	9,291	757,651
Belgium	10	10	23,382	191,789
Bulgaria	0	0	0	0
Croatia	0	0	0	0
Cyprus	0	0	0	0
Czech Republic	1	10	0	359,472
Denmark	0	3	0	58,355
Estonia	0	0	0	0
Finland	0	8	0	826,314
France	1	41	17,263	2,454,546
Germany	1	33	781	1,993,821

Greece	0	0	0	0
Hungary	0	12	0	605,894
Ireland	2	23	597	67,554
Italy	3	47	12,876	1,159,013
Latvia	0	0	0	0
Lithuania	0	0	0	0
Luxembourg	0	0	0	0
Malta	0	0	0	0
Netherlands	0	48	0	485,535
Poland	1	49	0	3,181,520
Portugal	0	3	0	60,739
Romania	0	14	17,899	1,688,857
Slovakia	0	0	0	0
Slovenia	0	0	0	0
Spain	0	68	34,636	5,458,592
Sweden	0	5	0	169,291
Iceland	0	0	0	0
Liechtenstein	0	0	0	0
Norway	0	5	0	313,944
Total EU	20	390	116,725	19,518,943

Total EEA	20	395	116,725	19,832,887
------------------	----	-----	---------	------------

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. Where an advertiser has violated an ad policy they are informed by way of a notification. This is visible in their TikTok Ads Manager account or, where an advertiser has booked their ad through a TikTok representative, then the representative will inform the advertiser of any violations. Advertisers are able to make use of functionality to appeal rejections of their ads in certain circumstances. Ads already on TikTok may go through an additional stage of review if certain conditions are met (e.g., reaching certain impression thresholds) or because of random sampling conducted at TikTok's own initiative.</p>			
SLI 2.4.1	<p>We are pleased to be able to share the number of appeals for ads removed under our Covid-19 misinformation and political content ad policies in this report.</p>			
	Number of appeals for ads removed under the covid 19 policy	Number of appeals for ads removed under political content policy	Number of overturn of appeals under the covid 19 policy	Number of overturn of appeal under political content policy
Member States				
Austria	0	11	0	5
Belgium	0	3	0	1
Bulgaria	0	0	0	0
Croatia	0	0	0	0
Cyprus	0	0	0	0
Czech Republic	0	4	0	0
Denmark	0	4	0	1

Estonia	0	0	0	0
Finland	0	4	0	0
France	0	8	0	0
Germany	0	8	0	2
Greece	0	0	0	0
Hungary	0	1	0	0
Ireland	0	7	0	0
Italy	0	8	0	1
Latvia	0	0	0	0
Lithuania	0	0	0	0
Luxembourg	0	0	0	0
Malta	0	0	0	0
Netherlands	0	3	0	0
Poland	0	8	0	2
Portugal	0	0	0	0
Romania	0	5	0	1
Slovakia	0	0	0	0
Slovenia	0	0	0	0
Spain	0	13	0	3
Sweden	0	2	0	1

Iceland	0	0	0	0
Liechtenstein	0	0	0	0
Norway	0	3	0	0
Total EU	0	89	0	17
Total EEA	0	92	0	17

II. Scrutiny of Ad Placements

Commitment 3

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

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	<ul style="list-style-type: none"> • Increased our alignment with IAB Sweden and Ireland, achieving Gold Standard certification in these countries. • Achieved the TAG Certified Against Fraud and TAG Brand Safety seals. • Continued to regularly participate in the working group on Ad Scrutiny.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes

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

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

III. Political Advertising Commitments 4 - 13

III. Political Advertising	
Commitment 4	
Relevant Signatories commit to adopt a common definition of “political and issue advertising”.	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	We have recently volunteered to co-chair the election working group and look forward to working with the other Signatories as part of this.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	We are keeping developments in the regulatory landscape under review and will carefully consider whether we need to implement any measures as a result of any changes.
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 4.1	
Measure 4.2	
QRE 4.1.1 (for measures 4.1 and 4.2)	<p>We prohibit political advertising, which is acknowledged to be a source of disinformation, with this Code dedicating a full Chapter to the topic of Political Advertising. Specifically, per our ads policies, we do not allow political actors to place advertising, nor do we allow ads and landing pages which:</p> <ul style="list-style-type: none"> • reference, promote, or oppose candidates or nominees for public office, political parties, or elected or appointed government officials; • reference an election, including voter registration, voter turnout, and appeals for votes;

	<ul style="list-style-type: none"> • include advocacy for or against past, current, or proposed referenda, ballot measures, and legislative, judicial, or regulatory outcomes or processes (including those that promote or attack government policies or track records); and • reference, promote, or sell, merchandise that features prohibited individuals, entities, or content, including campaign slogans, symbols, or logos <p>We allow cause-based advertising and public services advertising from government agencies, non-profits and other entities if they are not driven by partisan political motives.</p> <p>We also prohibit political content in branded content i.e. content which has been incentivised by a third party and needs to be disclosed in accordance with local advertising and consumer laws.</p> <p>We continue to monitor the evolution of the Proposal for an EU regulation on the transparency and targeting of political advertising (PAR) and are carefully considering any changes to our policies this might require.</p>
QRE 4.1.2 (for measures 4.1 and 4.2)	Not applicable at this stage.

III. Political Advertising	
Commitment 5	
Relevant Signatories commit to apply a consistent approach across political and issue advertising on their services and to clearly indicate in their advertising policies the extent to which such advertising is permitted or prohibited on their services.	
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].	Provided increased transparency for users and our stakeholders around our prohibition of political ads by disclosing new metrics.

Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	We are keeping developments in the regulatory landscape under review and will carefully consider whether we need to implement any measures as a result of any changes.
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 5.1	
QRE 5.1.1	Not applicable as TikTok does not allow political advertising.

III. Political Advertising	
Commitment 6	
Relevant Signatories commit to make political or issue ads clearly labelled and distinguishable as paid-for content in a way that allows users to understand that the content displayed contains political or issue advertising	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No
If yes, list these implementation measures here [short bullet points].	N/A
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	We are keeping developments in the regulatory landscape under review and will carefully consider whether we need to implement any measures as a result of any changes.

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

Measure 6.3	
QRE 6.3.1	Not applicable as TikTok does not allow political advertising.
Measure 6.4	
QRE 6.4.1	Not applicable as TikTok does not allow political advertising.
Measure 6.5	
QRE 6.5.1	Not committed. This commitment is not applicable as TikTok is not a messaging app.

III. Political Advertising

Commitment 7

Relevant Signatories commit to put proportionate and appropriate identity verification systems in place for sponsors and providers of advertising services acting on behalf of sponsors placing political or issue ads. Relevant signatories will make sure that labelling and user-facing transparency requirements are met before allowing placement of such ads.

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No
If yes, list these implementation measures here [short bullet points].	N/A
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	We are keeping developments in the regulatory landscape under review and will carefully consider whether we need to implement any measures as a result of any changes.
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 7.1	
QRE 7.1.1	Where accounts are designated as Government, Politician, and Political Party Accounts (“ GPPPA ”), those accounts are banned from placing ads on TikTok (with the exception of certain governmental entities) and from monetisation features. We publish the details of our GPPPA policy on our website , where we set out who we consider to be a GPPPA and make clear these restrictions on those types of account.
	N/A

SLI 7.1.1 – numbers for actions enforcing policies above (comparable metrics as for SLI 6.2.1)		
Member States	N/A	N/A

Total EU				
Total EEA				

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

III. Political Advertising

Commitment 8

Relevant Signatories commit to provide transparency information to users about the political or issue ads they see on their service.

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No
If yes, list these implementation measures here [short bullet points].	N/A
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	We are keeping developments in the regulatory landscape under review and will carefully consider whether we need to implement any measures as a result of any changes.
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 8.1	
Measure 8.2	
QRE 8.2.1 (for measures 8.1 & 8.2)	N/A

III. Political Advertising

Commitment 9

Relevant Signatories commit to provide users with clear, comprehensible, comprehensive information about why they are seeing a political or issue ad.

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No
If yes, list these implementation measures here [short bullet points].	N/A
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	We are keeping developments in the regulatory landscape under review and will carefully consider whether we need to implement any measures as a result of any changes.
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A
Measure 9.1	
Measure 9.2	
QRE 9.2.1 (for measures 9.1 & 9.2)	Not applicable as TikTok does not allow political advertising.

III. Political Advertising

Commitment 10

Relevant Signatories commit to maintain repositories of political or issue advertising and ensure their currentness, completeness, usability and quality, such that they contain all political and issue advertising served, along with the necessary information to comply with their legal obligations and with transparency commitments under this Code.

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	Launched the Commercial Content Library and made the Commercial Content API available to a limited number of researchers in preparation for the DSA.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Completing the full roll out of the Commercial Content Library and Commercial Content API in the EU.

Measure 10.1	
Measure 10.2	
QRE 10.2.1 (for measures 10.1 & 10.2)	Whilst we do not consider this provision applies to TikTok given TikTok bans political ads, we have launched the Commercial Content Library to comply with our obligations under the DSA. 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. It also includes information about content that is commercial in nature and tagged with either a paid partnership label or promotional label, such as content that promotes a brand, product or service, but that is not a paid ad (learn more on our Help Center).

III. Political Advertising	
Commitment 11	
Relevant Signatories commit to provide application programming interfaces (APIs) or other interfaces enabling users and researchers to perform customised searches within their ad repositories of political or issue advertising and to include a set of minimum functionalities as well as a set of minimum search criteria for the application of APIs or other interfaces.”	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	Launched the Commercial Content Library and made the Commercial Content API available to a limited number of researchers in preparation for the DSA.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes

<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<p>Completing the full roll out of the Commercial Content Library and Commercial Content API in the EU.</p>
<p>Measure 11.1</p>	
<p>Measure 11.2</p>	
<p>Measure 11.3</p>	
<p>Measure 11.4</p>	
<p>QRE 11.1.1 (for measures 11.1-11.4)</p>	<p>Whilst we do not consider this provision applies to TikTok given TikTok bans political ads, we launched the Commercial Content API, and tested with a limited number of researchers, to comply with our obligations under the DSA. We have built commercial content related APIs that includes ads, ad and advertiser metadata, 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.</p>
<p>QRE 11.4.1</p>	<p>We value feedback on where we can improve any of our APIs. We'll continue to respond with updates to better support independent research and transparency into TikTok.</p>

III. Political Advertising

Commitment 12

Relevant Signatories commit to increase oversight of political and issue advertising and constructively assist, as appropriate, in the creation, implementation and improvement of political or issue advertising policies and practices.

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No
If yes, list these implementation measures here [short bullet points].	TikTok did not subscribe to this commitment. Commitment 12 and associated measures are applicable to Civil Society only.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No
If yes, which further implementation measures do you plan to put in place in the next 6 months?	TikTok did not subscribe to this commitment. Commitment 12 and associated measures are applicable to Civil Society only.
Measure 12.1	
Measure 12.2	
Measure 12.3	
QRE 12.1.1 (for measures 12.1-12.3)	Commitment 12 and measures 12.1, 12.2 and 12.3 are applicable to Civil Society only.

III. Political Advertising

Commitment 13

Relevant Signatories agree to engage in ongoing monitoring and research to understand and respond to risks related to Disinformation in political or issue advertising.

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No
If yes, list these implementation measures here [short bullet points].	N/A
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	We are keeping developments in the regulatory landscape under review and will carefully consider whether we need to implement any measures as a result of any changes.
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A

Measure 13.1	
Measure 13.2	
Measure 13.3	
QRE 13.1.1 (for measures 13.1-13.3)	Whilst we do not allow political advertising, we are committed to remaining engaged with all discussions being held through the Task-force and other fora to ensure our policies and processes remain current and emerging and novel threats are addressed in our policies and enforcement.

IV. Integrity of Services Commitments 14 - 16

IV. Integrity of Services

Commitment 14

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

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

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

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

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

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"> • Carried out the most comprehensive updates to our CGs to date. Key changes made are set out in our Newsroom post and include more information about how we enforce certain policies and specific examples. • Launched our updated synthetic media policy to address the use of content created or modified by AI technology on our platform. • Continued to regularly participate in the working group on integrity of services.
<p>Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> • Continuing to strengthen how we enforce our synthetic media policy and exploring new products and initiatives to help enhance our detection and enforcement capabilities in relation to our synthetic media policy, including by developing a user education/outreach campaign. • Whilst we already have a number of policies in place which address hack and leak related threats, we are aiming to develop a more targeted response for certain risks related to this area. • As new deceptive behaviours emerge, we'll continue to evolve our response, strengthen enforcement capabilities and develop appropriate product and policy solutions.
<p>Measure 14.1</p>	

QRE 14.1.1

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

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

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

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

We do not allow spam including:

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

We also do not allow impersonation including:

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

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

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

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

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

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

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

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

Account hijacking or Impersonation

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

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

Deliberately targeting vulnerable recipients (e.g. via personalised advertising, location spoofing or obfuscation), inauthentic coordination of content creation or amplification,

including attempts to deceive/manipulate platforms algorithms (e.g. keyword stuffing or inauthentic posting/reposting designed to mislead people about popularity of content, including by influencers), use of deceptive practices to deceive/manipulate platform algorithms, such as to create, amplify or hijack hashtags, data voids, filter bubbles, or echo chambers and coordinated mass reporting of non-violative opposing content or accounts.

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

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

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

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

While we have a number of policies that address hack and leak related threats (some examples are below), as stated we have identified the use of hack and leak operations as an area for further policy development.

- Our CIOs addresses use of leaked documents to sway public opinion as part of a wider operation

- Our synthetic media policy captures materials that has been digitally altered without an appropriate disclosure
- Our harmful misinformation policies combats conspiracy theories related to unfolding events and dangerous misinformation
- Our Trade of Regulated Goods and Services policy prohibits trading of hacked goods

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

Our synthetic media policy requires **deceptive or synthetic media** that shows realistic scenes must be clearly disclosed (see our newsroom post, [here](#)).

For the purposes of our policy, synthetic media refers to content created or modified by AI technology. It includes highly realistic digitally-created (fake) content of real people, such as a video of a real person speaking but their words have been modified or changed.

In accordance with our policy, we prohibit:

- Synthetic media showing realistic scenes that are not prominently disclosed or labelled in the video
- Synthetic media that contains the likeness (visual or audio) of a real person, including: (1) a young person, (2) an adult private figure, and (3) an adult public figure when used for political or commercial endorsements, or if it violates any other policy
- Material that has been edited, spliced, or combined (such as video and audio) in a way that may mislead a person about real-world events

Non-transparent compensated messages or promotions by influencers

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

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* it is 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 use detection models and rule engines that:

- prevent inauthentic accounts from being created based on malicious patterns; and
- remove registered accounts based on certain signals (ie, 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 assessing and addressing identified violations.

In addition, where content reaches certain levels of popularity in terms of the number of video views, it will be flagged for further review. Such review is undertaken given the extent of the content's dissemination and the increase in potential harm if the content is found to be in breach of our CGs including our I&A policies.

We have also set up specifically-trained teams that are focused on investigating and detecting CIO on our Platform. When we investigate and remove these operations, we focus on behaviour and assessing linkages between accounts and techniques to determine if actors are engaging in a coordinated effort to mislead TikTok's systems or our community. In each case, we believe that the people behind these activities coordinate with one another to misrepresent who they are and what they are doing.

Measure 14.2

QRE 14.2.1

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

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

Where our teams have a high degree of confidence that an account amounts to an **impersonation**, or is engaged in or is connected to networks we took down in the past as part of a CIO, it is removed from our Platform. Please note that in relation to CIO, we are only able to provide data for Q4 2022 and Q1 2023. We are building and testing data infrastructure that can provide information requested at a high level of fidelity. Additionally, CIO investigations are highly resource heavy and require in-depth analysis to ensure high confidence in proposed actions.

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

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

SLI 14.2.1 – SLI 14.2.4

TTP OR ACTION1

TTP No. 1: Creation of inauthentic accounts or botnets (which may include automated, partially automated, or non-automated accounts)

Methodology of data measurement

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.

We have updated our methodology to report the monthly average of fake accounts as a percentage of monthly active users, in order to better reflect TTPs related content in relation to overall content on the service.

Due to data retention issues, we are unable to report data under this TTP for January and February 2023. As such, the following data covers the period of March to June 2023.

SLI 14.2.1

SLI 14.2.2

SLI 14.2.3

SLI 14.2.4

Nr of actions taken by type

Interaction/engagement before action

TTPs related content in relation to overall content on the service

List actions per member states (see example table above)		Number of fake accounts removed		Number of followers of fake accounts identified at the time of removal						Monthly average of Fake accounts as a % of monthly active users		
Member States												
Austria		37,432		1,0,153								
Belgium		171,151		1,730,851								
Bulgaria		21,804		660,538								
Croatia		9,983		281,371								
Cyprus		6,074		164,718								
Czech Republic		20,493		1,132,908								
Denmark		14,399		316,793								
Estonia		3,618		174,645								
Finland		18,064		364,796								
France		1,172,756		11,581,950								
Germany		1,304,861		6,514,711								

Greece		16,926		723,781								
Hungary		15,821		829,671								
Ireland		67,013		296,274								
Italy		1,334,235		6,912,898								
Latvia		8,892		200,801								
Lithuania		23,412		887,373								
Luxembourg		8,028		250,413								
Malta		3,078		63,625								
Netherlands		85,994		958,160								
Poland		46,679		2,399,891								
Portugal		30,965		405,402								
Romania		25,349		3,126,296								
Slovakia		9,246		356,935								
Slovenia		6,086		198,861								
Spain		1,306,958		5,016,793								
Sweden		116,641		358,979								
Iceland		64,649		416,202								

Liechtenstein		1,958		39,216								
Norway		27,052		1,284,990								
Total EU		5,885,958		47,409,587						1.10%		
Total EEA		5,979,617		49,149,995								

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
	Nr of actions taken by type	Interaction/ engagement before action		
List actions per member states (see example table above)	Number of fake likes removed	Number of fake likes prevented		
Austria	1,345,637	7,595,324		
Belgium	2,234,417	14,221,785		
Bulgaria	417,816	9,649,791		
Croatia	71,661	7,202,539		

Cyprus	191,587	1,936,645		
Czech Republic	365,385	7,306,804		
Denmark	535,378	4,992,195		
Estonia	105,870	4,644,054		
Finland	374,053	5,247,191		
France	7,832,363	211,067,472		
Germany	14,195,201	435,615,462		
Greece	567,815	17,800,053		
Hungary	337,974	6,371,084		
Ireland	726,720	8,503,276		
Italy	3,905,694	79,009,196		

Latvia	197,693	3,759,420		
Lithuania	137,300	2,731,025		
Luxembourg	222,688	2,026,143		
Malta	44,722	793,758		
Netherlands	2,593,567	27,786,721		
Poland	797,217	33,467,234		
Portugal	481,187	10,359,309		
Romania	1,682,208	25,056,279		
Slovakia	143,757	4,701,246		
Slovenia	88,822	2,729,128		
Spain	2,579,549	75,228,340		

Sweden	2,932,226	16,413,123		
Iceland	45,393	710,806		
Liechtenstein	983	325,029		
Norway	797,166	6,843,278		
Total EU	45,108,507	1,026,214,597		
Total EEA	45,952,049	1,034,093,710		

TTP OR ACTION 3	TTP No. 3: Use of fake followers or subscribers			
	Methodology of data measurement: We based the number of fake followers that we removed on the country of registration of the user. We also based the number of fake followers prevented on the country of registration of the user.			
	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4
	Nr of actions taken by type	Interaction/ engagement before action		
List actions per member states (see example table above)	Number of fake followers removed	Number of fake follows prevented		
Member States				
Austria	916,762	15,113,971		
Belgium	950,155	32,167,594		
Bulgaria	159,526	30,517,686		

Croatia	72,268	6,951,209		
Cyprus	72,230	3,794,578		
Czech Republic	313,609	53,084,383		
Denmark	288,523	17,990,193		
Estonia	56,409	4,152,796		
Finland	175,916	255,252,569		
France	5,585,542	354,544,000		
Germany	8,200,715	496,570,985		
Greece	296,210	33,711,467		
Hungary	140,336	17,953,492		
Ireland	218,158	26,034,349		
Italy	3,539,871	167,795,942		

Latvia	76,303	12,285,545		
Lithuania	78,443	17,715,602		
Luxembourg	75,418	8,581,244		
Malta	16,953	818,129		
Netherlands	1,592,720	150,970,651		
Poland	628,863	65,628,071		
Portugal	223,455	19,163,874		
Romania	793,756	101,484,888		
Slovakia	103,690	9,538,471		
Slovenia	30,516	3,162,979		
Spain	2,072,164	268,402,194		
Sweden	1,083,017	46,842,241		

Iceland	41,487	1,976,114		
Liechtenstein	4,043	67,393		
Norway	580,625	12,384,401		
Total EU	27,761,528	2,220,229,103		
Total EEA	28,387,683	2,234,657,011		

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

TTP OR ACTION 5	TTP No. 5: Account hijacking or impersonation			
	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 monthly average of impersonation accounts as a percentage of monthly active users as it better reflects the relation of the TTPs related content to overall content on the service			
SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4	
Nr of actions taken by type			TTPs related content in relation to overall content on the service	
Member States	Number of account banned under impersonation policy			Impersonation accounts as a % of monthly active users
List actions per member states (see example table above)				
Austria	157			
Belgium	370			
Bulgaria	225			
Croatia	29			
Cyprus	22			

Czech Republic	134			
Denmark	89			
Estonia	14			
Finland	84			
France	2,894			
Germany	1,629			
Greece	212			
Hungary	109			
Ireland	144			
Italy	703			
Latvia	12			
Lithuania	28			
Luxembourg	10			
Malta	4			
Netherlands	944			
Poland	1,069			
Portugal	139			

Romania	990			
Slovakia	43			
Slovenia	20			
Spain	588			
Sweden	197			
Iceland	7			
Liechtenstein	1			
Norway	166			
Total EU	10,859			0.0014%
Total EEA	11,033			

TTP OR ACTION 6	TTP No. 6. Deliberately targeting vulnerable recipients (e.g. via personalised advertising, location spoofing or obfuscation)						
	<p>Methodology of data measurement:</p> <p>The number of CIO networks targeting countries relates to the Q4 2022 and Q1 2023 period. We have categorised disrupted CIO networks by the country we assess that the network originated in. We have included any network which originated in Europe or that targeted one or more European countries. We publish all of the CIO networks we identify and remove within our transparency reports, here.</p> <p>The number of accounts linked to CIO networks identified and removed are based on the geographic location of network operation and technical and behavioural evidence from proprietary and open sources. The number of followers of CIO networks has been based on the number of accounts that followed any account within a network as of the date of that network's removal.</p>						
	SLI 14.2.1		SLI 14.2.2			SLI 14.2.3	SLI 14.2.4
Member States (Network origin)	Nr of instances of identified TTPs	Nr of actions taken by type	Interaction/engagement before action	Views/impressions after action	Interaction/engagement after action	Trends on targeted audiences	

Russia	3,181 accounts in the network	3,181 accounts removed	418,196 accounts followed an account within the network as at the date of removal	0	0	<p>The network targeted European countries, primarily Germany.</p> <p>The individuals behind these accounts created inauthentic accounts and shared inauthentic localised content in German about the ongoing war in Ukraine, as well as its consequences on EU countries' economies.</p>	
Poland	41 accounts in the network	41 accounts removed	40,256 accounts followed an account within the network as at the date of removal	0	0	<p>The network targeted Polish audiences.</p> <p>The individuals behind this network created inauthentic identities and hyper-posted comments with similar content in order to artificially promote anti-Russian viewpoints.</p>	

Russia	12 accounts in the network	12 accounts removed	1,480 accounts followed an account within the network as at the date of removal	0	0	<p>The network targeted various European countries such as Germany, Italy, and the UK.</p> <p>The individuals behind this network used impersonation in order to artificially amplify specific viewpoints related to Ukraine's president Zelensky, the economic sanctions currently imposed on Russia, and Ukrainian refugees.</p>	
Ireland	72 accounts in the network	72 accounts removed	94,743 accounts followed an account within the network as at the date of removal	0	0	<p>The network targeted Irish audiences.</p> <p>The individuals behind this network created inauthentic accounts; hyper-posted content with divisive views related to nationalism in Ireland, Japan, Russia, and Taiwan; and hyper-posted comments with similar low-quality content in an attempt to redirect TikTok users off-platform and to intensify social conflict.</p>	

Germany	6 accounts in the network	6 accounts removed	368,644 accounts followed an account within the network as at the date of removal	0	0	<p>The network targeted Egyptian audiences.</p> <p>The individuals behind this network created inauthentic accounts in order to artificially amplify calls to join non-existing protests in Egypt targeting discourse around the current Egyptian government.</p>	
----------------	---------------------------	--------------------	---	---	---	---	--

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

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

TTP OR ACTION 9	<p>TTP No. 9: Inauthentic coordination of content creation or amplification, including attempts to deceive/manipulate platforms algorithms (e.g. keyword stuffing or inauthentic posting/reposting designed to mislead people about popularity of content, including by influencers)</p> <p>We have provided data on the CIO networks that we have disrupted in the Q4 2022 and Q1 2023 period under TTP No. 6.</p>
------------------------	--

TTP OR ACTION 10	<p>TTP No. 10: Use of deceptive practices to deceive/manipulate platform algorithms, such as to create, amplify or hijack hashtags, data voids, filter bubbles, or echo chambers</p> <p>We have provided data on the CIO networks that we have disrupted in the Q4 2022 and Q1 2023 period under TTP No. 6.</p>
-------------------------	--

TTP OR ACTION 11	TTP No. 11. Non-transparent compensated messages or promotions by influencers			
	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4
	Methodology of data measurement: The branded content toggle allows users to self-disclose the existence of a commercial relationship. We have based the number of times the branded content toggle has been used on the approximate location of the users.			
	Nr of actions taken by type			
Member States				
List actions per member states (see example table above)	Number of times the branded content toggle has been used to disclose the existence of a commercial relationship			
Austria	45,504			
Belgium	84,288			
Bulgaria	37,025			
Croatia	12,140			
Cyprus	24,372			
Czech Republic	34,641			
Denmark	17,650			

Estonia	7,736			
Finland	18,298			
France	421,816			
Germany	468,614			
Greece	103,182			
Hungary	45,741			
Ireland	22,494			
Italy	305,252			
Latvia	70,413			
Lithuania	15,944			
Luxembourg	7,307			
Malta	6,207			
Netherlands	71,161			
Poland	155,680			
Portugal	120,180			
Romania	143,011			
Slovakia	14,555			
Slovenia	4,761			

Spain	352,719			
Sweden	46,266			
Iceland	0			
Liechtenstein	0			
Norway	20,597			
Total EU	2,656,957			
Total EEA	2,677,554			

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 Q4 2022 and Q1 2023 period under TTP No. 6.			
	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4
Member States				
List actions per member states (see example table above)				

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

IV. Integrity of Services

Commitment 15

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

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"> ● Launched our updated synthetic media policy to address the use of content created or modified by AI technology on our platform. ● As a launch partner of the Partnership on AI's (PAI) Responsible Practices for Synthetic Media, we contributed to the development of the relevant practices. ● We have joined new relevant groups when created, such as the Generative AI working group which will commence in September 2023.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	<ul style="list-style-type: none"> ● Continuing to strengthen how we enforce our synthetic media policy and exploring new products and initiatives to help enhance our detection and enforcement capabilities in relation to our synthetic media policy, including user education initiatives
Measure 15.1	

<p>QRE 15.1.1</p>	<p>We have updated our synthetic media policy to better address the use of content created or modified by AI technology on our platform (see our newsroom post, here). Under our I&A policies, we also prohibit other types of manipulated media that amount to harmful misinformation.</p> <p>While we welcome the creativity that new AI may unlock, in line with our updated policy, users must proactively disclose when their content is AI-generated or manipulated but shows realistic scenes (i.e. fake people, places or events that look like they are real). This can be done through the use of a sticker or caption, such as 'synthetic', 'fake', 'not real', or 'altered'. We do not allow:</p> <ul style="list-style-type: none"> ● synthetic media content which contains the likeness (visual or audio) of a real person - including: a young person, an adult private figure, and an adult public figure when used for political or commercial endorsements ● material that has been edited, spliced, or combined (such as video and audio) in a way that may mislead a person about real-world events. <p>We are currently developing a user education/outreach campaign in relation to this policy and are exploring products and initiatives to enhance our detection and enforcement capabilities.</p>
<p>Measure 15.2</p>	
<p>QRE 15.2.1</p>	<p>We have a number of measures to ensure the AI systems we develop uphold the principles of fairness and comply with applicable laws. To that end:</p> <ul style="list-style-type: none"> ● We have in place internal guidelines and training to help ensure that the training and deployment of our AI systems comply with applicable data protection laws, as well as principles of fairness. ● We have instituted a compliance review process for new AI systems that meet certain thresholds, and are working to prioritise review of previously developed algorithms. <p>We are proud to be a launch partner of the Partnership on AI's Responsible Practices for Synthetic Media. We contributed to developing the framework on how to responsibly develop, create, and share synthetic media.</p>

IV. Integrity of Services

Commitment 16

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

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	<ul style="list-style-type: none"> ● Actively engaged with the Crisis Response working group, proactively 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]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	<ul style="list-style-type: none"> ● Continuing to share relevant insights and metrics within our quarterly transparency reports, which aim to inform industry peers and the research community. ● Continuing to engage in the sub groups set up for insights sharing between signatories and the Commission. ● As new deceptive behaviours emerge, continuing to evolve our response, strengthen enforcement capabilities, develop appropriate product and policy solutions as appropriate.
Measure 16.1	

<p>QRE 16.1.1</p>	<p>Central to our strategy for identifying and removing CIO on our platforms is working with our stakeholders from civil society to user reports. This approach facilitates us - and others - disrupting the network's operations in their early stages. In addition to continuously enhancing our in-house capabilities, we proactively engage in comprehensive reviews of our peers' publicly disclosed findings and swiftly implement necessary actions in alignment with our policies.</p> <p>We share relevant insights and metrics within our quarterly transparency reports, which aim to inform industry peers and the research community.</p> <p>We continue to engage in the sub groups set up for insights sharing between signatories and the Commission. We are engaged with GARM at a local and a global level.</p>		
<p>SLI 16.1.1 Numbers of actions as a result of information sharing</p>	<p>N/A</p>		
<p>Data</p>			
<p>Measure 16.2</p>			
<p>QRE 16.2.1</p>	<p>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.</p>		

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].

- Carried out the most comprehensive updates to our CGs to date. Key changes made are set out in our [Newsroom post](#) and include more detail about how we protect civic and election integrity and use informational labels, warnings, and opt-in screens to increase transparency for our users.
- Scaled up our detection and labelling of state-controlled media accounts following the expansion of our state-controlled media label policy globally in [January 2023](#). Continued our extensive in-app interventions (including video tags, search interventions and in-app information hubs) in 23 official EU languages (plus for EEA users, Norwegian and Icelandic) around Covid-19, Covid-19 Vaccine, Holocaust Denial, Monkey Pox and the War in Ukraine. Launched a new search intervention on climate change to redirect users to trusted sources and encourage them to report any potential misinformation on the topic.
- Developed and launched eight localised media literacy campaigns addressing disinformation related to the war on Ukraine in PL, SK, RO, UA, HU, EE, LT, and LV, in close collaboration with our fact-checking partners.
- In the context of our commitment to promoting election integrity, we ran an Election Speaker Series and invited regional experts to present their insights in advance of the 2023 Spanish election, for which we launched an in-app campaign, using our intervention tools to connect users to authoritative information sources. We launched similar in-app campaigns in Greece and Finland in relation to their elections. We have also participated in the elections sub-group.
- Since August 2023, we have been notifying creators when their content has been made ineligible for recommendation and enabling them to appeal. We have also undertaken work to improve transparency in relation to our [appeals processes](#).

<p>Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> ● Continuing the detection and labelling of state-controlled media in Europe and expanding the policy further globally. ● Continuing to work with our fact-checking partners to identify local harmful misinformation trends in specific countries and develop tailored, localised media literacy campaigns to tackle such trends. ● Rolling out three media literacy campaigns in Europe in partnership with our trusted fact-checking partners based on topics identified in collaboration with our partners as priority areas for increasing the digital literacy of our users. ● Promoting election integrity in the run up to EU elections (including the upcoming Polish and Slovakian elections) by continuing to invite regional experts to share insights as part of our Election Speaker Series and launching additional in-app election campaigns to direct users to authoritative information. ● Continuing to explore ways to expand the use cases of our unverified content label. ● Exploring the addition of a toggle to facilitate users disclosing synthetic media
<p>Measure 17.1</p>	

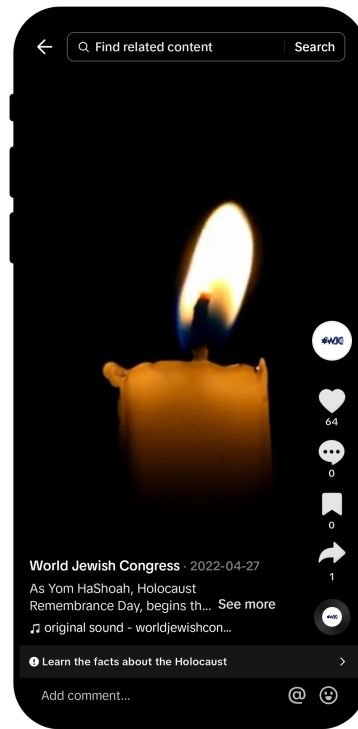
QRE 17.1.1

Together with systematically removing content from our platform that violates our I&A policies, we continue to dedicate significant resources to increasing the number of in-app measures that show users additional context on certain content or redirect them to authoritative information and to making those tools available in 23 EU official languages (plus, for EEA users, Norwegian, Icelandic).

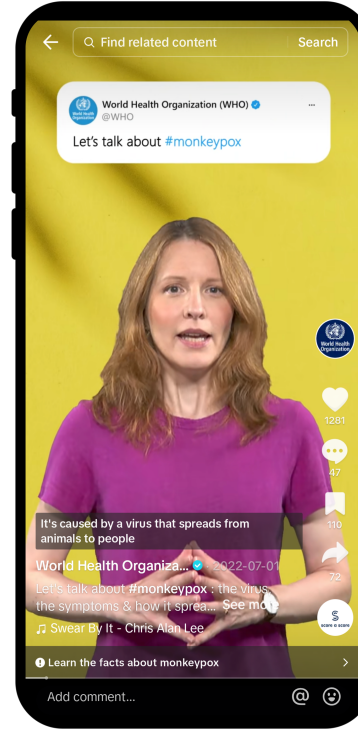
We work with external experts (e.g. World Health Organisation (**WHO**) on medical information) and our fact checker partners, and we take into account their feedback, as well as user feedback, in order to continually identify new topics and consider which tools may be best suited for raising awareness around that topic and combating harmful misinformation.

Since 2020, on topics such as [Covid-19](#), [Covid-19 Vaccine](#), [Holocaust Denial](#), MonkeyPox and War in Ukraine, we deployed a combination of a number of in-app intervention tools:

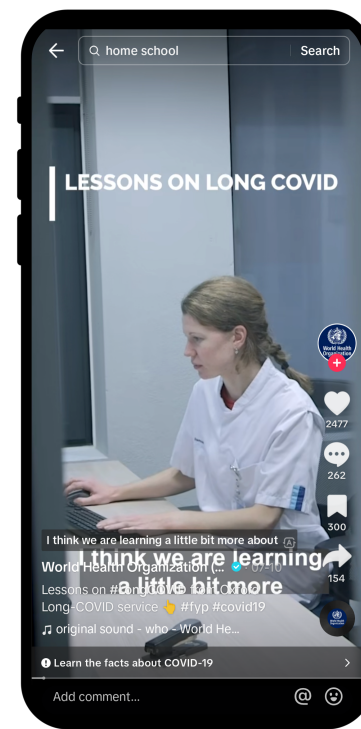
- **video notice tags.** These tags are applied to videos containing words or hashtags for the topic. The tag, which will invite the user to “*Learn more about* [the topic]”, is clickable and will redirect the user to a trusted resource page.



Holocaust Facts Video Notice Tag



Monkeypox Video Notice Tag

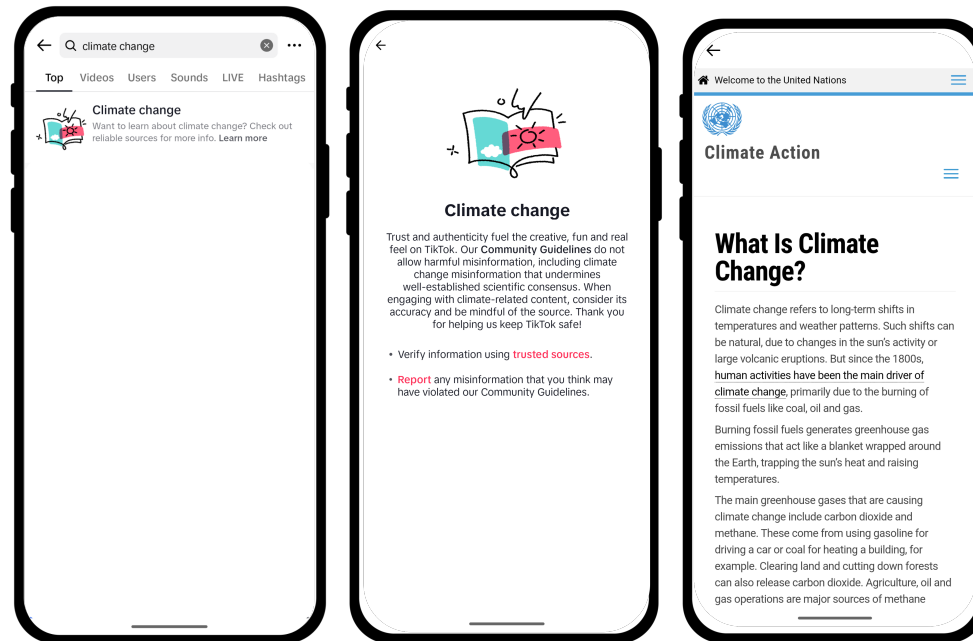


Covid-19 Video Notice Tag

- **search intervention.** If a user searches for keywords related to the topic, the user will be displayed a banner which may encourage them to verify the facts and will provide a link to a resource page. If the search term is violative, the user will not be displayed results and instead redirected to a trusted resource page.
- **public service announcement.** If a user searches for a hashtag on the topic, the user will be displayed a public service announcement that will remind users about our CG's and present them with links to trusted resource pages.
- **online and in-app information hubs and safety centre pages.** The above tools will often link to resource page(s) which direct users to accurate and up-to-date information from trusted sources. Depending on the topic or EU country involved, the user could

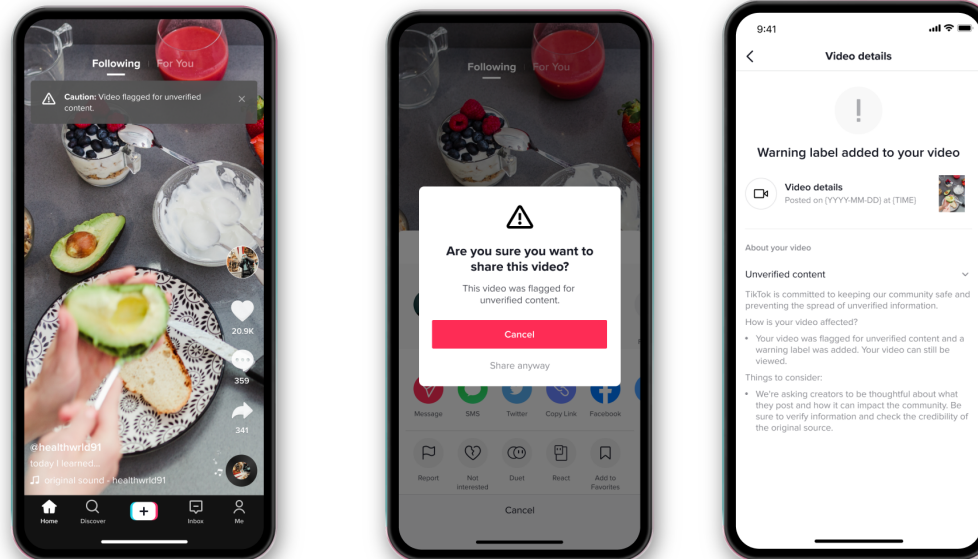
be directed to an external authoritative source (e.g., a national government website), an in-app information hub (e.g., War on Ukraine) or to a dedicated page on our safety centre website (e.g., [Covid-19](#) and [Elections integrity](#)).

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



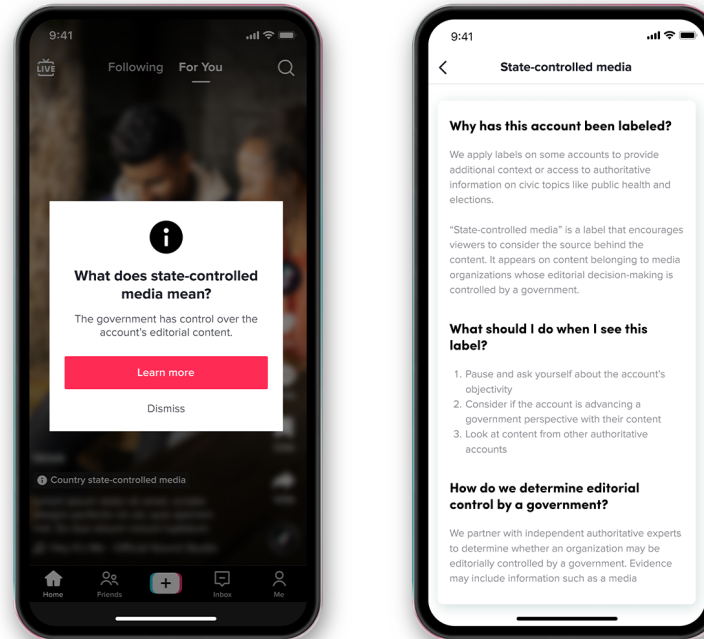
As well as the tools we deploy to increase users' digital citizenship regarding specific topics, we also apply warning labels to content related to unfolding or emergency events, irrespective of the topic, in order to encourage users to consider the reliability of the content or the source. These labels are available to users in 23 EU official languages (plus, for EEA users, Norwegian, and Icelandic). In our latest CG [update](#), we have further increased transparency for users around our use of warning labels.

- **Unverified content label.** To raise users' awareness about the credibility of content and to encourage people to reconsider sharing such content, we add warning labels to content related to unfolding or emergency events, including content which has been assessed by our fact-checkers but cannot be verified as accurate (see our newsroom post [here](#)).
 - The video will become ineligible for recommendation into anyone's For You feed to limit the spread of potentially misleading information.
 - The video's creator is also notified that their video was flagged as unsubstantiated content and is provided additional information about why the warning label has been added to their content. This is again to raise the creator's awareness about the credibility of the content that they have shared.



- **State affiliated media label.** In the EU, Iceland and Liechtenstein, we have taken steps to restrict access to content from Russia Today, Sputnik, Rossiya RTR / RTR Planeta, Rossiya 24 / Russia 24 and TV Centre International. We apply a prominent label to all other content or accounts from state affiliated media. The user is also automatically shown a full screen pop-up providing the user with information about what the label means and inviting the user to click on "learn more" and be redirected to an [in-app page](#). The measure brings transparency to our community and raises awareness among users to encourage users to consider the reliability of the source.

We continue to work with experts to inform our global approach and expansion and have expanded its use to media entities [globally](#).



We use our [Safety Center](#), which was designed following consultation with users, to inform our community about our approach to safety, privacy, and security on our platform. Relating to combating harmful misinformation, we have pages on:

- [Safety Partners](#): This section provides details of some of TikTok's work with industry experts, non-governmental organisations, and industry associations around the world in our commitment to building a safe platform for our community.
- **Specific topics**: With helpful resources such as [Online challenges](#) and [Elections integrity](#).

	<p>Users are able to learn more about our transparency efforts on our dedicated Transparency Center, which houses our historical transparency reports, including the reports we have published under the Code.</p> <p>We also use our Newsroom posts to communicate with our community transparently and to build and maintain trust. We continue to publish a range of posts in our Newsroom in which we seek, among other things, to generate awareness on safety and content related issues for example, recently we provided an overview of our refreshed CGs and introduced users to our climate change policy and search intervention.</p>		
SLI 17.1.1 - actions enforcing policies above	<p>Methodology of data measurement:</p> <p>The number of impressions, clicks and click through rates of video notice tags, search interventions and public service announcements are based on the approximate location of the users that engaged with the tools. The number of impressions of the Safety Center pages is based on the IP location of the users.</p> <p>For this reporting period, we are pleased to be able to report on engagement data for our state affiliated media label and data for the climate change search intervention. The latter was launched in April 2023 and the data presented only covers the three months period.</p>		
	Total count of the tool's impressions	Interactions/ engagement with the tool	Other relevant metrics
	Number of impressions of the State Affiliated Media label (SAM)	Number of clicks of the State Affiliated Media label (SAM)	Numbers of clicks through rate of the Stated Affiliate Media label (SAM)
Member States			
Austria	1,015,281	1,995	0.20%
Belgium	1,152,151	2,098	0.18%
Bulgaria	6,332,772	10,953	0.17%
Croatia	409,657	845	0.21%
Cyprus	236,436	417	0.18%
Czech Republic	1,337,856	2,490	0.19%

Denmark	455,326	1,464	0.32%
Estonia	336,898	1,052	0.31%
Finland	703,246	3,415	0.49%
France	7,861,637	13,888	0.18%
Germany	14,741,937	23,821	0.16%
Greece	1,245,885	2,936	0.24%
Hungary	13,775,641	13,148	0.10%
Ireland	660,375	2,193	0.33%
Italy	5,358,248	6,329	0.12%
Latvia	570,810	1,163	0.20%
Lithuania	648,253	1,637	0.25%
Luxembourg	110,808	198	0.18%
Malta	134,124	286	0.21%
Netherlands	4,374,341	7,613	0.17%
Poland	95,823,100	89,922	0.09%
Portugal	574,046	1,688	0.29%
Romania	5,540,229	12,510	0.23%
Slovakia	759,075	1,189	0.16%
Slovenia	229,969	386	0.17%
Spain	2,226,208	2,944	0.13%

Sweden	1,584,688	4,063	0.26%
Iceland	80,206	185	0.23%
Liechtenstein	2,061	0	0.00%
Norway	1,183,398	2,968	0.25%
Total EU	168,198,997	210,643	0.13%
Total EEA	169,464,662	213,796	0.13%
	Number of impressions of Video Notice Tag covered by Intervention (Covid-19)	Number of clicks of Video Notice Tag covered by Intervention (Covid-19)	Click Through Rate of Video Notice Tag covered by Intervention (Covid-19)
Member States			
Austria	36,724,542	41,874	0.11%
Belgium	39,347,820	59,136	0.15%
Bulgaria	14,558,553	14,817	0.10%
Croatia	11,742,126	9,419	0.08%
Cyprus	4,261,210	6,490	0.15%
Czech Republic	23,113,550	30,748	0.13%
Denmark	17,005,028	8,774	0.05%
Estonia	4,468,506	5,031	0.11%
Finland	20,908,974	26,339	0.13%
France	231,662,924	365,615	0.16%

Germany	352,687,850	385,620	0.11%
Greece	34,792,766	47,212	0.14%
Hungary	26,279,939	33,895	0.13%
Ireland	46,227,731	64,155	0.14%
Italy	322,681,950	475,453	0.15%
Latvia	7,050,794	7,950	0.11%
Lithuania	8,341,556	8,539	0.10%
Luxembourg	2,830,294	4,145	0.15%
Malta	2,491,790	3,488	0.14%
Netherlands	69,540,656	96,891	0.14%
Poland	85,487,642	100,268	0.12%
Portugal	24,518,581	40,918	0.17%
Romania	66,338,201	91,583	0.14%
Slovakia	11,495,418	8,429	0.07%
Slovenia	6,514,539	8,063	0.12%
Spain	266,356,197	448,756	0.17%
Sweden	43,927,850	68,986	0.16%
Iceland	2,116,365	3,343	0.16%
Liechtenstein	32,235	87	0.27%

Norway	25,353,278	13,451	0.05%
Total EU	1,781,356,987	2,462,594	0.14%
Total EEA	1,808,858,865	2,479,475	0.14%
	Number of impressions of Video Notice Tag covered by Intervention (Covid-19 Vaccine)	Number of clicks of Video Notice Tag covered by Intervention (Covid-19 Vaccine)	Click Through Rate of Video Notice Tag covered by Intervention (Covid-19 Vaccine)
Member States			
Austria	10,731,088	10,445	0.10%
Belgium	11,320,262	14,078	0.12%
Bulgaria	4,294,135	6,100	0.14%
Croatia	2,382,192	2,587	0.11%
Cyprus	974,213	1,330	0.14%
Czech Republic	4,004,472	5,043	0.13%
Denmark	3,142,432	3,822	0.12%
Estonia	668,118	775	0.12%
Finland	4,358,336	4,538	0.10%
France	70,443,046	101,901	0.14%
Germany	81,134,881	103,259	0.13%
Greece	9,519,339	12,044	0.13%
Hungary	5,283,159	6,657	0.13%

Ireland	17,606,949	9,392	0.05%
Italy	102,297,870	184,914	0.18%
Latvia	1,159,320	1,344	0.12%
Lithuania	1,560,536	1,670	0.11%
Luxembourg	598,347	1,011	0.17%
Malta	493,016	891	0.18%
Netherlands	16,850,066	20,176	0.12%
Poland	24,044,475	24,512	0.10%
Portugal	8,016,416	13,417	0.17%
Romania	20,474,032	19,786	0.10%
Slovakia	1,979,734	2,875	0.15%
Slovenia	1,165,069	1,368	0.12%
Spain	86,654,530	138,412	0.16%
Sweden	10,113,342	11,747	0.12%
Iceland	295,777	451	0.15%
Liechtenstein	2,198	20	0.91%
Norway	5,049,436	5,113	0.10%
Total EU	501,269,375	704,094	0.14%
Total EEA	506,616,786	709,678	0.14%

	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	7,449,512	13,293	0.18%
Belgium	9,618,327	19,192	0.20%
Bulgaria	1,660,909	4,368	0.26%
Croatia	1,342,982	3,197	0.24%
Cyprus	601,447	1,413	0.23%
Czech Republic	6,889,790	18,059	0.26%
Denmark	4,252,268	8,625	0.20%
Estonia	556,576	1,363	0.24%
Finland	5,544,295	12,222	0.22%
France	51,784,760	107,713	0.21%
Germany	58,510,763	96,942	0.17%
Greece	5,181,231	13,466	0.26%
Hungary	7,270,568	14,611	0.20%
Ireland	7,671,588	13,560	0.18%
Italy	57,918,699	153,245	0.26%
Latvia	595,952	1,279	0.21%

Lithuania	1,309,387	3,288	0.25%
Luxembourg	401,105	1,030	0.26%
Malta	308,516	664	0.22%
Netherlands	17,170,706	31,336	0.18%
Poland	35,881,393	84,624	0.24%
Portugal	5,257,400	19,321	0.37%
Romania	9,262,167	26,071	0.28%
Slovakia	1,425,447	3,607	0.25%
Slovenia	1,145,274	2,291	0.20%
Spain	16,557,183	56,465	0.34%
Sweden	10,627,334	24,298	0.23%
Iceland	451,978	1,218	0.27%
Liechtenstein	10,521	11	0.10%
Norway	6,201,917	13,128	0.21%
Total EU	326,195,579	735,543	0.23%
Total EEA	332,859,995	749,900	0.23%
	Number of impressions of Video Notice Tag covered by Intervention (Monkey Pox)	Number of clicks of Video Notice Tag covered by Intervention (Monkey Pox)	Click Through Rate of Video Notice Tag covered by Intervention (Monkey Pox)
Member States			

Austria	138,635	599	0.43%
Belgium	154,074	688	0.45%
Bulgaria	86,880	187	0.22%
Croatia	28,002	105	0.37%
Cyprus	19,271	67	0.35%
Czech Republic	46,665	176	0.38%
Denmark	157,841	1,268	0.80%
Estonia	13,216	27	0.20%
Finland	295,210	875	0.30%
France	723,102	1,007	0.14%
Germany	1,800,643	5,878	0.33%
Greece	104,485	296	0.28%
Hungary	80,108	403	0.50%
Ireland	93,134	198	0.21%
Italy	371,564	987	0.27%
Latvia	13,571	32	0.24%
Lithuania	24,317	69	0.28%
Luxembourg	8,409	20	0.24%
Malta	8,690	14	0.16%

Netherlands	354,080	2,130	0.60%
Poland	339,557	840	0.25%
Portugal	119,028	617	0.52%
Romania	215,663	514	0.24%
Slovakia	27,884	81	0.29%
Slovenia	19,053	30	0.16%
Spain	770,945	1,792	0.23%
Sweden	272,867	1,429	0.52%
Iceland	4,967	22	0.44%
Liechtenstein	102	1	0.98%
Norway	105,940	482	0.45%
Total EU	6,286,894	20,329	0.32%
Total EEA	6,397,903	20,834	0.33%
	Number of impressions of Search interventions (Covid-19)	Number of clicks of Search interventions (Covid-19)	Click Through Rate of Search interventions (Covid-19)
Member States			
Austria	17,119	245	1.43%
Belgium	37,754	457	1.21%
Bulgaria	13,421	285	2.12%

Croatia	10,798	157	1.45%
Cyprus	4,404	72	1.63%
Czech Republic	23,842	243	1.02%
Denmark	14,449	164	1.14%
Estonia	4,195	80	1.91%
Finland	23,020	231	1.00%
France	291,716	2,799	0.96%
Germany	149,614	2,094	1.40%
Greece	36,783	459	1.25%
Hungary	32,750	453	1.38%
Ireland	63,448	467	0.74%
Italy	538,680	7,263	1.35%
Latvia	7,041	132	1.87%
Lithuania	8,270	178	2.15%
Luxembourg	2,196	38	1.73%
Malta	2,659	32	1.20%
Netherlands	60,403	666	1.10%
Poland	141,570	842	0.59%
Portugal	68,172	1,072	1.57%

Romania	68,034	1,154	1.70%
Slovakia	11,179	153	1.37%
Slovenia	5,384	78	1.45%
Spain	542,883	9,289	1.71%
Sweden	51,334	601	1.17%
Iceland	2,414	21	0.87%
Liechtenstein	38	0	0.00%
Norway	23,099	294	1.27%
Total EU	2,231,118	29,704	1.33%
Total EEA	2,256,669	30,019	1.33%
	Number of impressions of Search interventions (Covid-19 Vaccine)	Number of clicks of Search interventions (Covid-19 Vaccine)	Click Through Rate of Search interventions (Covid-19 Vaccine)
Member States			
Austria	20,851	149	0.71%
Belgium	4,624	24	0.52%
Bulgaria	2,690	15	0.56%
Croatia	3,186	26	0.82%
Cyprus	1,160	21	1.81%
Czech Republic	9,078	59	0.65%

Denmark	3,377	15	0.44%
Estonia	672	5	0.74%
Finland	3,688	9	0.24%
France	29,250	139	0.48%
Germany	217,286	1,332	0.61%
Greece	5,945	28	0.47%
Hungary	4,827	17	0.35%
Ireland	14,193	24	0.17%
Italy	124,749	764	0.61%
Latvia	1,181	9	0.76%
Lithuania	2,274	21	0.92%
Luxembourg	708	9	1.27%
Malta	601	5	0.83%
Netherlands	12,102	78	0.64%
Poland	11,989	47	0.39%
Portugal	28,189	128	0.45%
Romania	22,869	147	0.64%
Slovakia	2,606	19	0.73%
Slovenia	1,254	3	0.24%

Spain	19,346	84	0.43%
Sweden	16,690	78	0.47%
Iceland	603	3	0.50%
Liechtenstein	34	0	0.00%
Norway	6,736	55	0.82%
Total EU	565,385	3,255	0.58%
Total EEA	572,758	3,313	0.58%
	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	150,954	5,467	3.62%
Belgium	132,598	4,258	3.21%
Bulgaria	64,803	1,610	2.48%
Croatia	73,667	2,336	3.17%
Cyprus	19,028	446	2.34%
Czech Republic	120,393	3,402	2.83%
Denmark	75,709	1,734	2.29%
Estonia	14,434	501	3.47%
Finland	138,485	2,621	1.89%

France	505,541	18,561	3.67%
Germany	1,190,140	60,945	5.12%
Greece	479,073	5,495	1.15%
Hungary	116,042	4,410	3.80%
Ireland	129,544	2,564	1.98%
Italy	548,733	17,645	3.22%
Latvia	16,092	764	4.75%
Lithuania	46,679	1,124	2.41%
Luxembourg	9,884	381	3.85%
Malta	4,731	176	3.72%
Netherlands	360,128	7,542	2.09%
Poland	379,830	641	0.17%
Portugal	151,062	2,382	1.58%
Romania	199,281	5,045	2.53%
Slovakia	54,201	1,602	2.96%
Slovenia	17,676	630	3.56%
Spain	558,465	30,747	5.51%
Sweden	192,764	5,365	2.78%
Iceland	6,100	231	3.79%

Liechtenstein	229	11	4.80%
Norway	106,638	2,853	2.68%
Total EU	5,749,937	188,394	3.28%
Total EEA	5,862,904	191,489	3.27%
	Number of impressions of Search interventions (Monkey Pox)	Number of clicks of Search interventions (Monkey Pox)	Click Through Rate of Search interventions (Monkey Pox)
Member States			
Austria	1,327	7	0.53%
Belgium	808	4	0.50%
Bulgaria	348	3	0.86%
Croatia	212	0	0.00%
Cyprus	109	0	0.00%
Czech Republic	367	3	0.82%
Denmark	591	0	0.00%
Estonia	107	2	1.87%
Finland	888	3	0.34%
France	3,077	7	0.23%
Germany	9,668	28	0.29%
Greece	754	0	0.00%

Hungary	329	7	2.13%
Ireland	628	4	0.64%
Italy	2,305	19	0.82%
Latvia	116	0	0.00%
Lithuania	281	5	1.78%
Luxembourg	82	0	0.00%
Malta	34	0	0.00%
Netherlands	1,840	7	0.38%
Poland	1,028	5	0.49%
Portugal	1,771	0	0.00%
Romania	1,204	3	0.25%
Slovakia	128	0	0.00%
Slovenia	40	0	0.00%
Spain	1,765	8	0.45%
Sweden	2,184	3	0.14%
Iceland	51	0	0.00%
Liechtenstein	5	0	0.00%
Norway	1,064	5	0.47%
Total EU	31,991	118	0.37%

Total EEA	33,111	123	0.37%
	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	66,088	32	0.05%
Belgium	29,228	18	0.06%
Bulgaria	12,494	19	0.15%
Croatia	13,546	4	0.03%
Cyprus	2,638	6	0.23%
Czech Republic	19,085	15	0.08%
Denmark	19,718	19	0.10%
Estonia	3,318	6	0.18%
Finland	25,034	26	0.10%
France	116,881	95	0.08%
Germany	714,604	316	0.04%
Greece	32,177	48	0.15%
Hungary	28,395	25	0.09%
Ireland	36,485	17	0.05%
Italy	155,423	166	0.11%

Latvia	4,303	7	0.16%
Lithuania	8,582	13	0.15%
Luxembourg	2,801	3	0.11%
Malta	1,677	1	0.06%
Netherlands	56,372	36	0.06%
Poland	82,423	73	0.09%
Portugal	47,277	24	0.05%
Romania	42,318	63	0.15%
Slovakia	9,555	17	0.18%
Slovenia	4,245	8	0.19%
Spain	122,701	85	0.07%
Sweden	79,740	51	0.06%
Iceland	965	3	0.31%
Liechtenstein	75	0	0.00%
Norway	30,388	25	0.08%
Total EU	1,737,108	1,193	0.07%
Total EEA	1,768,536	1,221	0.07%
	Number of impressions of Public service announcements (Covid-19)	Number of impressions of Public service announcements (Covid 19 Vaccine)	Number of impressions of Public service announcements (Holocaust Misinformation/Denial)

Member States			
Austria	35,449,004	3,906,370	860
Belgium	21,990,634	8,588,282	1,110
Bulgaria	10,010,605	2,516,279	429
Croatia	7,638,300	2,259,323	608
Cyprus	2,705,288	1,124,607	110
Czech Republic	11,430,855	2,377,188	974
Denmark	10,107,551	2,548,794	932
Estonia	2,691,001	779,204	213
Finland	13,425,322	3,464,911	1,182
France	117,035,776	81,780,870	3,272
Germany	356,128,744	34,170,321	5,882
Greece	22,959,418	8,408,221	1,245
Hungary	13,311,875	4,832,469	1,103
Ireland	19,880,647	8,549,551	1,226
Italy	153,031,278	62,442,165	13,439
Latvia	4,317,180	1,216,632	278
Lithuania	5,288,323	1,269,161	395
Luxembourg	2,014,856	606,363	96

Malta	1,351,257	556,946	68
Netherlands	49,052,814	9,855,994	1,953
Poland	53,148,519	9,456,435	2,492
Portugal	11,780,851	2,302,900	457
Romania	41,032,339	23,523,542	1,416
Slovakia	5,657,147	1,765,056	509
Slovenia	3,968,805	1,349,807	288
Spain	99,941,238	14,158,130	1,579
Sweden	25,493,176	9,009,808	2,213
Iceland	1,074,458	336,799	200
Liechtenstein	68,976	10,324	1
Norway	14,519,963	3,939,479	1,351
Total EU	1,100,842,803	302,819,329	44,329
Total EEA	1,116,506,200	307,105,931	45,881
	Number of impressions of Public service announcements (Monkey Pox)	Number of impressions of the safety center page on Covid-19	Number of impressions of the safety center page on election integrity
Member States			
Austria	6	7,601	851
Belgium	39	10,785	1,059

Bulgaria	5	16,250	1,534
Croatia	6	3,576	154
Cyprus	1	1,692	159
Czech Republic	2	5,101	443
Denmark	12	2,829	205
Estonia	1	809	53
Finland	22	5,633	548
France	48	82,207	8,011
Germany	54	101,999	10,310
Greece	10	9,495	1,001
Hungary	7	6,781	507
Ireland	7	9,904	1,797
Italy	36	47,314	3,793
Latvia	1	3,790	135
Lithuania	1	3,997	163
Luxembourg	1	1,120	93
Malta	0	2,808	55
Netherlands	28	26,395	2,311
Poland	18	17,203	1,426

Portugal	4	7,760	450
Romania	16	38,134	3,149
Slovakia	4	2,826	243
Slovenia	0	1,391	90
Spain	38	44,703	3,223
Sweden	36	10,934	1,032
Iceland	0	415	23
Liechtenstein	0	27	1
Norway	9	4,072	366
Total EU	403	473,037	42,795
Total EEA	412	477,551	43,185

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

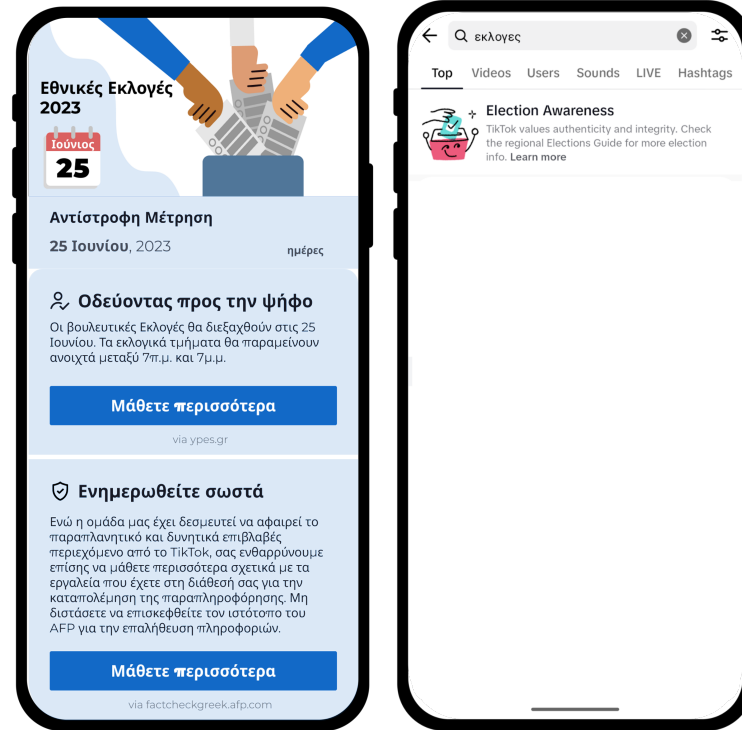
QRE 17.2.1

In order to raise awareness among our users of 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) in that we collaborate with national partners and use language that the local audience can best connect with. For other campaigns such as the War on Ukraine, our emphasis is on connecting users to scalability, safety and helpful resources.

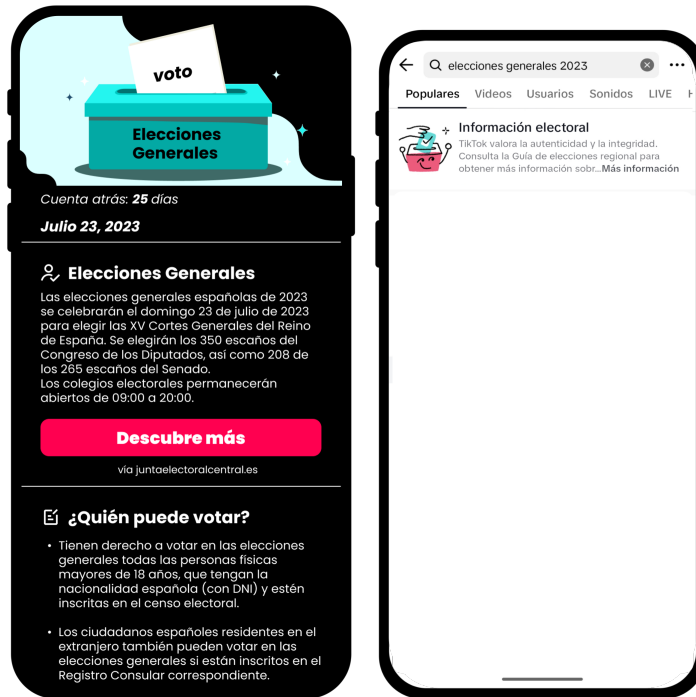
Below are examples of the campaigns we have most recently run in-app which have leveraged a number of the intervention tools (e.g. search interventions and video notice tags) we have outlined in our response to QRE 17.1.1.

(I) Promoting election integrity. As well as the [elections integrity page](#) within TikTok's Safety Center to bring visibility to how we're protecting our platform from harmful misinformation and foreign interference, we've launched media literacy campaigns in advance of several European major elections.

- **2023 Finnish election.** From 6 March 2023, we launched a search guide to provide users with up to date information about the Finnish election. We partnered with The National Audiovisual Institute and linked users to their Media Literacy [website](#).
- **2023 Greek election.** From 3 May 2023, we rolled out a campaign, consisting of a search intervention and in-app Election Hub in advance of the May Greek election (see screenshots, below). The Election Hub connected users to authoritative information sources and encouraged users to educate themselves on misinformation via AFP's Greek Fact Check [page](#). We continued the campaign in the lead up to the second Greek election held on 25 June.



- **2023 Spanish election.** We launched a search intervention and in-app election hub to provide users with up to date information in advance of the Spanish general election which took place on 23 July 2023. We worked with Newtral, our fact-checking partner, and Maldita, a local media literacy organisation, to produce educational videos about the electoral process and election misinformation



We also organise Election Speaker Series in the lead-up to certain elections, and recently did so for the 2023 Spanish general election. As part of this, we invite suitably qualified external local/regional experts to share their insights and market expertise with our internal teams in order to inform our approach to the upcoming election. Thus as part of TikTok's preparations for the Spanish election on 23rd July, our local fact-checking partner Newtral was engaged to provide a Speaker Series presentation.

(III) War in Ukraine. Working with our fact-checking partners, this year we have developed and rolled-out eight localised media literacy campaigns on the war in [Poland](#), Slovakia, Romania, Ukraine, Hungary, Estonia, Latvia and Lithuania. Users searching for keywords relating to the war are directed to tips, prepared in partnership with our fact checking partners, to help users identify misinformation and prevent the spread of it on the platform.

	<p>(IV) Covid-19. We implemented a comprehensive campaign across a number of jurisdictions to address disinformation related to Covid-19. Our dedicated notice tags and search intervention tools now direct users to authoritative, localised information from expert organisations (such as local public health sites or, where local health sites are not available, the WHO).</p> <p>We have ambitious plans to continue to develop and roll out media literacy campaigns this year in partnership with our trusted fact-checking partners based on topics identified in collaboration with our partners as priority areas for increasing the digital literacy of our users.</p>			
SLI 17.2.1 - actions enforcing policies above	<p>We are pleased to report metrics for our Polish media literacy campaign in partnership with Fakenews.pl. The campaign was launched in March 2023 and the following data covers the 4 months period since its launch.</p> <p>We have also recently launched separate campaign in Slovakia, Romania, Ukraine, Hungary, Estonia, Latvia and Lithuania and we will include this data in the following report.</p>			
	Number of ads run for media literacy campaign	Number of impressions of the media literacy ads	Number of clicks on the media literacy ads	Click Through Rate of the media literacy ads
Member States				
Poland	3	31,390,354	54701	0.24%
	Number of users that received the push notification	Number of clicks on the push notification	Click Through Rate on the push notification	
Poland	2,753,933	62,401	2.27%	

Measure 17.3	
QRE 17.3.1	<p>As outlined in our Safety Partners page within TikTok's Safety Center, we partner with experts on many areas including on media literacy campaigns including to collaborate on the development of the campaign and to direct users to their authoritative resources. Our experts include fact-checkers, academics, NGOs and government entities. Specific examples of partnerships within the campaigns and projects set out in QRE 17.2.1 are:</p> <p>(I) Promoting election integrity. We partner with various media organisations and fact-checkers in the context of our election campaigns. For more detail about the input our fact-checking partners provide please refer to QRE 30.1.3.</p> <ul style="list-style-type: none"> • For the Finnish elections, we partnered with The National Audiovisual Institute and linked users to their Media Literacy website. • For our search intervention and in-app Election Hub for the 2023 Greek elections, we worked with our fact checking partner Agence France Press and linked users to its Greek Fact Check page. <p>(II) War in Ukraine. We launched our Polish war in Ukraine campaign in partnership with Fakenews.pl, a local organisation which specialises in Russian disinformation. Our campaigns in Slovakia, Romania, Ukraine, Hungary, Estonia, Latvia and Lithuania were launched in partnership with Lead Stories.</p> <p>(III) Covid-19. In relation to Covid-19 misinformation, we have continued our partnerships with: (i) the WHO Tech Taskforce; and (ii) our European fact-checkers including AFP, Facta, Logically, Lead Stories, Newtral, Science Feedback, Teyit, DPA and Reuters (who we have recently onboarded in Europe). Our partners provide us with information about Covid-19 trends including new variants, vaccine side effects on adults and children, and information about new treatments (such as antivirals). This information helps us improve our in-app intervention tools.</p>

V. Empowering Users

Commitment 18

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

<p>In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]</p>	<p>Yes</p>
<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> ● Continued to scale our fact-checking program by adding coverage in nine additional EEA countries (Denmark, Finland, Norway, Greece, Cyprus, Belgium, Czech Republic, Slovakia, and Bulgaria) and expanding our misinformation moderation teams in those languages accordingly. ● Continued to detect and label state-controlled media accounts following the roll out of our state-controlled media label policy across globally in January 2023 ● Strengthened machine learning models in GR, CY, FI, NO, DK and BE as part of our investments to tackle harmful misinformation ● Committed to participating in a data access pilot with EDMO in order to trial the process for sharing data with vetted researchers as designated under the DSA ● Invested in training and development for our Trust and Safety team, by partnering with subject matter experts such as Yad Vashem, who created an enrichment program to help the team develop a deeper understanding of conspiracy theories and misinformation related to the Holocaust. ● Engaged with the research community on a range of topics, including elections, climate misinformation, AI, hack and leak operations and media literacy campaigns. These consultations inform policy and feature development. ● Continued to participate in, and co-chair, the working group on Elections.
<p>Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]</p>	<p>Yes</p>

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

- Continued expansion of our fact-checking network, consisting of committing to onboarding new European-based fact-checking partners and increasing our operational coverage in the EEA (and expanding our misinformation moderation teams accordingly).
- Continuing to strengthen machine learning models in further EEA countries as we expand our fact-checking coverage.
- Continuing to explore ways to expand the use cases of our unverified content label.
- Continue investing in training and development for our Trust and Safety team with the help of our fact-checking partners and external experts in this field, including by continuing to launch Election Speaker Series in advance of major EU elections.
- Continuing to participate in, and co-chair, the working group on Elections.

Measure 18.1

QRE 18.1.1

We work hard to reduce the spread of harmful misinformation that could mislead our community about civic processes, public health, or safety regardless of intent. Our approach to safety is systemic and spans policies, product, practices, and partners.

(I) Removal of violating content or accounts. We aim to remove content or accounts that violate our CGs including our I&A policies before they are viewed or shared by other people in order to reduce potential harm. Content on TikTok first goes through technology that reviews it against our guidelines. Assessing harmful misinformation may require additional context and assessment by our specialized misinformation moderators who have enhanced training, expertise and tools to identify such content, including direct access to our fact-checking partners.

If content is identified as a potential violation, it will be automatically removed, or flagged for additional review by our trust & safety team. Additional review will occur if a video gains popularity or has been reported. Community members can report violations in-app and on our website. Our fact-checking partners and other stakeholders can also report potential violating content to us.

Our Trust and Safety teams can detect and remove harmful misinformation *before* it is reported to us by users or third parties effectively because we place considerable emphasis on proactive moderation. Videos uploaded to TikTok are initially reviewed by our automated moderation technology, which look at a variety of signals across content, including keywords, images, titles, descriptions and audio, to identify violating content. We also carry out targeted sweeps of certain types of violative content including harmful misinformation, where we have identified specific risks or where our fact-check partners or other experts have alerted us to specific risks. We may also issue guidance to our moderation teams to help them more easily spot and take swift action on violating content.

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

- a. For content that does not violate our CGs but may negatively impact the authenticity of the platform, we reduce its prominence on the For You feed and / or label it. The types of misinformation we may make For You feed

ineligible are now made even clearer to users [here](#); general conspiracy theories, unverified information related to emergencies and unfolding events and potential high-harm misinformation that is undergoing a fact check. We also label accounts and content of state affiliated media entities to empower users to consider the sources of information. Our safety team takes additional precautions to review videos as they rise in popularity to reduce the likelihood of content that may not be appropriate entering our recommended system.

- b. Providing access to authoritative information is an important part of our overall strategy to counter misinformation. There are a number of ways in which we do this, including launching information centers with informative resources from authoritative third-parties in response to global or local events, adding public service announcements on hashtag or search pages, or labelling content related to a certain topic to prompt our community to seek out authoritative information.

(III) design by safety. Within our Trust and Safety team, we have individuals in product and policy and subject matter experts dedicated to the topic of integrity and authenticity. In developing a new feature or policy, these teams our Trust and Safety team work closely with external partners to incorporate their expertise and ensure we are reflecting industry best practice. For example:

- We collaborated with [Irrational Labs](#) to develop and implement [specialised prompts](#) to help users consider before sharing unverified content (as outlined in **QRE 21.3.1**),
- [Yad Vashem](#) created for TikTok an enrichment program on the Holocaust for our Trust and Safety team. The five week programme aimed to give our team a deeper understanding about the Holocaust, its lessons and misinformation related to antisemitism and hatred.
- We work with local/regional election experts to share their insights and expertise with our internal teams in the lead up to EU elections (as outlined in **QRE 17.3.1**).

QRE 18.1.2

The For You feed is the interface users first see when they open TikTok. It's central to the TikTok experience and where most of our users spend their time exploring the platform. The system recommends content by ranking videos based on a combination of factors including:

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

All these factors are weighted based on their value to a user and the recommendation system then ranks them to determine the likelihood of a user’s interest in a particular category of content. The weighting of a factor can change dynamically. We share more information about our recommender system below in our response to QRE 19.1.1.

QRE 18.1.3

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 I&A policies make clear that we do not allow activities that may undermine the integrity of our platform or the authenticity of our users. We remove content or accounts that involve misleading information that causes significant harm or, in certain circumstances, reduce the prominence of content. The types of misinformation we may make ineligible For You feed are now made even clearer to users [here](#); namely, general conspiracy theories, unverified information related to emergencies or unfolding events and potential high-harm misinformation that is undergoing a fact check. To enforce our CGs at scale, we use a combination of technology and moderation teams. Assessing harmful misinformation requires additional context and assessment by our specialized misinformation moderators who have enhanced training, expertise and tools to identify such content, including direct access to our fact-checking partners.

Working with our network of independent fact-checking organisations, enable TikTok to identify potential misinformation, take action on it, and share accurate information with our community around important events. Our fact-checking partners do not moderate content on our platform, but their assessments provide valuable input which helps us take the appropriate action that upholds our CGs. In addition to reporting on and assessing potential misinformation, TikTok partners with professional fact-checkers to improve our detection and enforcement on misinformation through:

- a proactive detection program with our fact-checkers who flag new and evolving claims they're seeing across the internet. This allows us to look for these claims on our platform and remove violations.
- a database of previously fact-checked claims to help misinformation moderators make swift and accurate decisions.

Providing access to authoritative information is an important part of our overall strategy to counter misinformation. There are a number of ways in which we do this, including launching information centers with informative resources from authoritative third-parties in response to global or local events, adding public service announcements on hashtag or search pages, or labelling content related to a certain topic to prompt our community to seek out authoritative information.

	We also invest in combatting content designed to mislead our community about elections. We work with electoral commissions and civic society organizations to help ensure that we're providing our community with access to trustworthy and relevant information through in-app election centers, search interventions, content labels and hashtag PSAs.			
SLI 18.1.1 - actions proving effectiveness of measures and policies	Methodology of data measurement:			
	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.			
				Other relevant metrics
List actions per member states and languages (see example table above)				Share cancel rate (%) following the unverified content label share warning pop-up (users who do not share the video after seeing the pop up)
Member States				
Austria				31.80%
Belgium				29.60%
Bulgaria				35.44%
Croatia				40.00%
Cyprus				44.44%

Czech Republic				40.48%
Denmark				20.83%
Estonia				28.21%
Finland				20.00%
France				28.89%
Germany				31.69%
Greece				39.86%
Hungary				30.36%
Ireland				33.82%
Italy				36.79%
Latvia				37.50%
Lithuania				28.89%
Luxembourg				27.59%
Malta				33.33%
Netherlands				27.59%
Poland				29.00%
Portugal				26.06%

Romania				29.98%
Slovakia				30.00%
Slovenia				15.38%
Spain				30.73%
Sweden				23.36%
Iceland				66.67%
Liechtenstein				0.00%
Norway				22.41%
Total EU				29.93%
Total EEA				29.92%

Measure 18.2

QRE 18.2.1

As stated, to help keep our platform welcoming and authentic for everyone, we take seriously ensuring the content on our platform is free from harmful misinformation.

Our I&A policies within our CGs and Terms of Service 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 guidelines make clear to our users what content we remove or make ineligible for the For You feed when they pose a risk of harm to our users and their communities. We recently refreshed our CGs, in order to provide increased transparency to our users on our policies and more detailed examples. CGs are also explained to our users in a series of user-friendly, colourful [videos](#) in our Safety Center.

As is made clear in our CGs, we do not allow inaccurate, misleading, or false content that may cause significant harm to individuals or society regardless of intent.

Specifically, our policies do not allow:

- Misinformation that poses a risk to public safety or may induce panic about a crisis event or emergency.
- Medical misinformation, such as misleading statements about vaccines, inaccurate medical advice that discourages people from getting appropriate medical care for a life-threatening disease, and other misinformation that poses a risk to public health.
- Climate change misinformation that undermines well established scientific consensus, such as denying the existence of climate change or the factors that contribute to it.
- Dangerous conspiracy theories that are violent or hateful.
- Specific conspiracy theories that name and attack individual people.
- Material that has been edited, spliced, or combined (such as video and audio) in a way that may mislead a person about real-world events.
- Election misinformation.

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

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

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

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

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

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

However, misinformation is different from other content issues. Context and fact-checking are critical to consistently and accurately enforcing our misinformation policies. So while we use machine learning models to help detect potential misinformation, ultimately our approach today is having our moderation team assess, confirm, and remove misinformation violations. We have specialised misinformation moderators who have enhanced training, expertise, and tools to take action on harmful misinformation. This includes direct access to our fact-checking partners who help assess the accuracy of content.

We strive to maintain a balance between freedom of expression and protecting our users and the wider public from harmful content. Our approach to combating harmful misinformation, as stated in our CGs, is to remove content that is both false and can cause harm to individuals or

	<p>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 unfolding events, the video may not be removed and may instead become ineligible for recommendation into anyone's For You feed to limit the spread of potentially misleading information and labelled with the “unverified content” label.</p> <p>We are pleased to include in this report the number of videos made ineligible for the For You feed under the relevant I&A policies (general conspiracy theories and unverified information related to an emergency or unfolding event) as disclosed here to users.</p> <p>Note that in relation to the metrics we have shared at SLI 18.2.1 below, of all the views that occurred in H1 2023, fewer than 2 in 10,000 views occurred on content identified and removed for violating our policies around harmful misinformation.</p>			
<p>SLI 18.2.1 - actions taken in response to policy violations</p>	<p>Methodology of data measurement:</p> <p>We have based the following numbers on the country in which the video was posted: videos removed because of violations of our harmful misinformation policies.</p> <p>The number of views of videos removed because of violation of each of the harmful misinformation policies is based on the approximate location of the user.</p>			
<p>List actions per member states and languages (see example table above)</p>	<p>Total no of violations</p>	<p>Metric 1: indicating the impact of the action taken</p>	<p>Total no of violations</p>	<p>Metric 1: indicating the impact of the action taken</p>
	<p>Number of videos removed because of violation of harmful misinformation policy</p>	<p>Number of views of videos removed because of violation of harmful misinformation policy</p>	<p>Number of videos made ineligible for the For You feed under the relevant I&A policies (general)</p>	

			conspiracy theories and unverified information related to an emergency or unfolding event)	
Member States				
Austria	1,097	9,625,250	542	
Belgium	2,115	15,719,128	4	
Bulgaria	171	7,647,804	214	
Croatia	52	1,464,537	13	
Cyprus	204	1,682,932	0	
Czech Republic	932	13,467,903	180	
Denmark	466	16,160,341	136	
Estonia	28	1,051,117	11	
Finland	459	10,048,892	54	
France	30,677	156,328,751	18,570	
Germany	18,747	319,588,907	8,253	
Greece	1,217	18,105,562	427	

Hungary	437	11,282,377	155	
Ireland	2,165	2,440,995	15	
Italy	45,510	81,210,621	10,160	
Latvia	18	2,339,276	8	
Lithuania	43	2,194,918	3	
Luxembourg	13	848,454	2	
Malta	3	0	7	
Netherlands	2,624	20,778,184	2,117	
Poland	4,157	83,042,521	1,931	
Portugal	448	10,929,050	86	
Romania	4,656	93,214,915	2,592	
Slovakia	402	11,039,156	121	
Slovenia	33	324,949	3	
Spain	20,493	107,118,504	26,916	
Sweden	3,468	14,365,855	1,795	
Iceland	21	102,276	3	
Liechtenstein	0	0	0	

Norway	2,055	7,629,680	141	
Total EU	140,635	1,012,020,899	74,315	
Total EEA	142,711	1,019,752,855	74,459	
Measure 18.3				
QRE 18.3.1	<p>We regularly consult with third party experts and researchers in relation to the development of policies and features which are designed to reduce the spread of disinformation. Over the last six months we have engaged with the research community on a range of relevant topics, including elections, climate misinformation, AI, hack and leak operations, and media literacy campaigns. These consultations directly inform our policy and feature development.</p> <p>We are proud of our close work with behavioural psychologists, Irrational Labs, which led to the development of the following warning and labelling features more detail at QRE 21.3.1):</p> <ul style="list-style-type: none"> • specialised prompts for unverified content, which alerts viewers to unverified content identified during unfolding events and • our state affiliated media label, which brings transparency to our community in relation to state affiliated media entities and raises awareness among users to encourage users to consider the reliability of the source. <p>We are exploring ways in which we can leverage consultations carried out with researchers from the Massachusetts Institute of Technology (US) and the University of Regina (Canada) about the design of tools which would facilitate engagement with users who have interacted with harmful misinformation on our platform (more detail at QRE 21.2.1).</p> <p>We are proud to be a launch partner of the Partnership on AI's Responsible Practices for Synthetic Media. We contributed to developing the framework on how to responsibly develop, create, and share synthetic media.</p>			

V. Empowering Users

Commitment 19

Relevant Signatories using recommender systems commit to make them transparent to the recipients regarding the main criteria and parameters used for prioritising or deprioritising information, and provide options to users about recommender systems, and make available information on those options.

<p>In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]</p>	<p>Yes</p>
<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> • Improved user transparency of the way in which our recommender systems operate. See our updated Help Center article here. • Rolled-out a new feature that enables users to refresh their For You feed if their recommendations no longer feel relevant. • Since August 2023, in the context of our obligations under the DSA (Article 38), introduced non-personalized feeds on our platform, which provide users with an alternative to recommender systems which are based on profiling. See here.
<p>Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> • Continuing to explore ways in which we increase transparency for users around our recommender systems including exploring developing a dedicated online safety hub

Measure 19.1	
QRE 19.1.1	<p>The For You feed is the interface users first see when they open TikTok. It's central to the TikTok experience and where most of our users spend their time exploring the platform.</p> <p>We make clear to users in our Terms of Service and CGs (and also provide more context in our Help Center article) 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 CGs, we take steps to avoid recommending certain categories of content that may not be appropriate for a broad audience including general conspiracy theories and unverified information related to an emergency or unfolding event. We may also make some of this content harder to find in search</p> <p>Main parameters. The system recommends content by ranking videos based on a combination of factors including:</p> <ul style="list-style-type: none"> ● user selections (i.e. interest categories indicated in the registration process or selecting “not interested” on content); ● user interactions (i.e. videos users like/share, watch in full or skip accounts users follow, accounts that follow users, comments users post and content they create); ● video information (i.e. captions/sounds and hashtags used, number of video views, and the country in which the video was published.); and ● device and account settings (i.e. language preferences, country settings, time zone and day, and device types). <p>All these factors are weighted based on their value to a user and the recommendation system then ranks them to determine the likelihood of a user's interest in a particular category of content. The weighting of a factor can change dynamically. If a user watches a longer video from beginning to end, this would be considered a strong indicator of interest and receive a greater weight than a weak indicator such as device and account settings because users don't actively express these preferences. If a viewer never finishes watching any videos, but watches a lot of videos posted by creators in the same region, then that region may have a relatively stronger weight compared to other factors for that viewer. These predictions are also influenced by the interactions of other people on TikTok who appear to have similar interests. For example, if a user likes videos 1, 2, and 3 and a second user likes videos 1, 2, 3, 4 and 5, the recommendation system may predict that the first user will also like videos 4 and 5.</p>

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

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.

- Users can click on any video and select “not interested” to automatically skip future videos from that same creator or using the same audio.
- Users are able to automatically filter out videos with specific words or hashtags associated with content that they don't want to see from their For You or Following feeds (see [here](#)).
- Users can enable “[Restricted Mode](#)” within their account settings in order to limit the appearance of content that may not be appropriate for all audiences.
- As part of our efforts to meet DSA requirements, we are giving our European community another way to discover content on TikTok. They will be able to turn off personalisation so that their For You and LIVE feeds will instead show the most popular videos in their regions and internationally, rather than recommending content to them based on their personal interests (see [here](#)).
- Users are able to [refresh their For You feed](#) if their recommendations no longer feel relevant. When the feed is refreshed, users view content on their For You feed as if they have just signed up for TikTok. Our recommendation system will then begin to surface more content based on new interactions.

We overhauled the design of the Safety Center website to make it more colourful and to use more images and graphics and created a series of longer length videos to bolster our efforts to communicate with users via a variety of media formats. Thus, as well as providing this information to users in our Terms of Service and CGs, we have created a [series of informative videos](#) specifically on the For You feed and our recommendation system. Users can also browse through the top [questions](#) we get asked on our recommendation systems and our answers.

	As well as making clear to users how the recommender system works, we have established our Transparency and Accountability Centers , where there's an opportunity to get even more detail on how our recommendation systems work.			
Measure 19.2				
SLI 19.2.1 – user settings	Methodology of data measurement:			
	The number of users who have filtered hashtags or a keyword to set preferences for For You feed, the number of times a user clicks “not interested” in relation to the For You feed, and the number of times users clicked on the For You Feed Refresh are all based on the approximate location of the users that engaged with these tools.			
	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	
Member States				
Austria	25,250	1,112,238	17,303	
Belgium	32,133	1,576,718	15,108	
Bulgaria	15,952	813,331	5,782	
Croatia	10,178	428,836	3,190	
Cyprus	2,966	197,568	1,897	
Czech Republic	21,829	1,037,009	4,134	

Denmark	17,515	662,731	4,653	
Estonia	5,858	187,409	1,752	
Finland	19,699	840,032	7,090	
France	151,018	11,123,013	75,534	
Germany	246,381	11,686,883	165,509	
Greece	27,594	1,422,886	10,171	
Hungary	23,441	1,177,879	5,656	
Ireland	26,777	964,388	8,437	
Italy	133,706	7,834,427	43,060	
Latvia	7,435	293,439	3,073	
Lithuania	10,109	347,298	3,723	
Luxembourg	2,314	114,388	1,247	
Malta	1,369	86,178	780	
Netherlands	68,100	3,255,389	25,511	
Poland	102,540	4,392,201	21,864	
Portugal	28,200	1,273,345	11,033	
Romania	42,976	3,218,205	33,654	
Slovakia	9,287	400,110	2,136	
Slovenia	4,919	189,680	1,591	
Spain	130,051	7,457,391	86,269	

Sweden	41,860	1,775,909	16,728	
Iceland	2,370	66,217	492	
Liechtenstein	92	2,901	53	
Norway	24,479	853,769	4,077	
Total EU	1,209,457	63,868,881	576,885	
Total EEA	1,236,398	64,791,768	581,507	

V. Empowering Users

Commitment 20

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

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No
If yes, list these implementation measures here [short bullet points].	TikTok did not subscribe to this commitment. TikTok considers that it would be imprudent to commit to this measure at a time when the underlying technology remains unproven and the standards to be complied with are not yet finalised.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No
If yes, which further implementation measures do you plan to put in place in the next 6 months?	N/A

Measure 20.1	
QRE 20.1.1	Not committed. TikTok considers that it would be imprudent to commit to this measure at a time when the underlying technology remains unproven and the standards to be complied with are not yet finalised. Once the relevant technology is proven and the standards are agreed and identifiable, TikTok will assess whether such an approach would be beneficial, taking into account existing measures in place.
Measure 20.2	
QRE 20.2.1	Not committed. Similarly to Measure 20.1, TikTok considers that it would be imprudent to commit to this measure at this time. TikTok is, however, open to reassessing in the future whether such an approach would be beneficial.

V. Empowering Users	
Commitment 21	
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.	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	<ul style="list-style-type: none"> Continued to scale-up our fact-checking program by adding coverage in nine additional EEA countries (Denmark, Finland, Norway, Greece, Cyprus, Belgium, Czech Republic, Slovakia, and Bulgaria) and expanding our misinformation moderation teams in those languages. Completed consultations with researchers from the Massachusetts Institute of Technology (US) and the University of Regina (Canada) to consider how we engage

	<p>with users who have interacted with harmful misinformation on our platform and direct them to authoritative information.</p> <ul style="list-style-type: none"> • Developed and launched a new in-app search intervention on climate change to redirect users to trusted information on the topic. • Exploring the addition of a toggle to facilitate users disclosing synthetic media.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	<ul style="list-style-type: none"> • Following consultations with researchers, exploring and considering how we engage with users who have interacted with harmful misinformation on our platform and direct them to authoritative information. • Continuing to explore ways to expand the use cases of our unverified content label. • Continued expansion of our fact-checking network, consisting of committing to onboarding new European-based fact-checking partners and increasing our operational coverage in the EEA (and expanding our misinformation moderation teams accordingly).
Measure 21.1	
QRE 21.1.1	<p>We currently have 9 IFCN accredited fact checking organisations providing coverage in Europe, in 17 of the official European languages. Our response to QRE 30.1.2 sets out the specific organisations we partner with.</p> <p>We ensure that our users benefit from the context and insights provided by the fact checking organisations we partner with in the following ways:</p> <ul style="list-style-type: none"> • Enforcement of misinformation policies. Our fact-checking partners play a critical role in helping us enforce our misinformation policies, which aim to promote a trustworthy and authentic experience for our users. We consider context and fact-checking to be key to consistently and accurately enforcing these policies, so, while we use machine learning models to help detect potential misinformation, we have our specialised misinformation

moderators assess, confirm, and take action on harmful misinformation. As part of this process, our moderators are able to provide content to our expert fact checking partners for further evaluation. Where fact checkers advise that content is false, our moderators take measures to assess and remove it from our platform. Our response to QRE 31.1.1 provides further insight into the way in which fact-checkers are involved in this process.

- **Unverified content labelling.** Our fact-checkers support certain of the in-app tools we have designed in order to bring users additional context on certain content or provide access to authoritative information. As mentioned above, we partner with fact checkers to assess the accuracy of content. Sometimes, our fact-checkers determine that content is not able to be confirmed or checks are inconclusive (especially during unfolding events or crises). Where our fact-checkers provide us with an inconclusive/ unconfirmed determination, we use our unverified content label to inform viewers [via a banner](#) that a video contains 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.
- **In-app tools related to specific topics:**
 - **Covid-19.** We partnered with a number of fact checkers throughout the EU in order to prevent the spread of harmful misinformation related to Covid-19 on our platform, including AFP, Facta, Logically, Lead Stories, Newtral, Science Feedback, Teyit and DPA.
 - **Election integrity.** We have launched campaigns in advance of several major elections aimed at educating the public about the voting process which encourage users to fact-check information with our fact-checking partners. The election integrity campaign we rolled out in advance of the Italian general election included setting up an in-app [Elections Center](#) to connect people who engage with election content with our fact checkers, e.g., [Facta.news](#). We launched the campaign with a [blog post](#) that introduced the Election Center and explained our content labelling and fact-checking processes.
 - **Climate Change.** We recently launched a search intervention which redirects users seeking out climate change-related content to authoritative information. We worked with the UN to provide the authoritative information (see our newsroom post [here](#)).

	<ul style="list-style-type: none"> • User awareness of our fact-checking partnerships and labels. We have published blog posts (available in more than 25 languages) and created a hub on our Safety Center to raise users' awareness of our fact-checking programme and labels and to support the work of our fact checking partners. 				
SLI 21.1.1 - actions taken under measure 21.1	<p>Methodology of data measurement:</p> <p>The share of removals under our harmful misinformation policy, share of proactive removals, share of removals before any views and share of the removals within 24h are relative to total removals under our CGs.</p> <p>The share cancel rate (%) following the unverified content label share warning pop-up indicates the percentage of users who do not share a video after seeing the label pop up. This metric is based on the approximate location of the users that engaged with these tools.</p>				
	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 harmful 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	31.80%	0.59%	0.51%	0.54%	0.20%
Belgium	29.60%	0.66%	0.77%	0.81%	0.51%

Bulgaria	35.44%	0.06%	0.01%	0.01%	0.03%
Croatia	40.00%	0.09%	0.07%	0.05%	0.06%
Cyprus	44.44%	0.70%	0.71%	0.76%	0.48%
Czech Republic	40.48%	0.37%	0.04%	0.03%	0.21%
Denmark	20.83%	0.38%	0.33%	0.41%	0.30%
Estonia	28.21%	0.07%	0.06%	0.06%	0.04%
Finland	20.00%	0.22%	0.16%	0.20%	0.14%
France	28.89%	1.45%	1.57%	2.05%	1.39%
Germany	31.69%	0.89%	0.81%	0.67%	0.12%
Greece	39.86%	0.39%	0.33%	0.29%	0.27%
Hungary	30.36%	0.19%	0.10%	0.09%	0.15%
Ireland	33.82%	0.69%	0.72%	0.84%	0.35%
Italy	36.79%	2.30%	2.37%	2.70%	2.41%
Latvia	37.50%	0.03%	0.01%	0.01%	0.02%
Lithuania	28.89%	0.07%	0.04%	0.05%	0.05%
Luxembourg	27.59%	0.05%	0.05%	0.06%	0.02%
Malta	33.33%	0.02%	0.02%	0.03%	0.02%
Netherlands	27.59%	0.25%	0.24%	0.24%	0.21%
Poland	29.00%	0.20%	0.15%	0.15%	0.17%
Portugal	26.06%	0.21%	0.15%	0.12%	0.14%

Romania	29.98%	0.53%	0.46%	0.39%	0.36%
Slovakia	30.00%	0.44%	0.06%	0.05%	0.22%
Slovenia	15.38%	0.10%	0.08%	0.09%	0.07%
Spain	30.73%	1.29%	1.33%	1.60%	1.29%
Sweden	23.36%	0.91%	0.99%	1.19%	0.83%
Iceland	66.67%	0.21%	0.02%	0.03%	0.08%
Liechtenstein	0.00%	0.00%	0.00%	0.00%	0.00%
Norway	22.41%	1.47%	1.61%	1.51%	0.85%
Total EU	29.93%	0.93%	0.93%	1.01%	0.78%
Total EEA	29.92%	0.94%	0.94%	1.01%	0.78%

SLI 21.1.2 - actions taken under measure 21.1	Methodology of data measurement:			
	<p>The number of videos tagged with the unverified content label is based on the country in which the video was posted.</p> <p>The share cancel rate (%) following the unverified content label share warning pop-up indicates the percentage of users who do not share a video after seeing the label pop up. This metric is based on the approximate location of the users that engaged with these tools.</p>			
		Nr of labels applied to content, such as on the basis of such articles		Meaningful metrics such as the impact of 21.1. measures on user interactions with, or user re-shares of, content fact-checked as false or misleading

List actions per member states and languages (see example table above)		Number of videos tagged with the unverified content label		Share cancel rate (%) following the unverified content label share warning pop-up (users who do not share the video after seeing the pop up)
Member States				
Austria		2,772		31.80%
Belgium		4,169		29.60%
Bulgaria		1,404		35.44%
Croatia		611		40.00%
Cyprus		587		44.44%
Czech Republic		1,168		40.48%
Denmark		985		20.83%
Estonia		681		28.21%
Finland		923		20.00%
France		14,003		28.89%
Germany		9,776		31.69%
Greece		1,443		39.86%
Hungary		913		30.36%
Ireland		2,216		33.82%
Italy		5,770		36.79%
Latvia		952		37.50%

Lithuania		763		28.89%
Luxembourg		761		27.59%
Malta		355		33.33%
Netherlands		4,414		27.59%
Poland		3,627		29.00%
Portugal		2,136		26.06%
Romania		2,026		29.98%
Slovakia		625		30.00%
Slovenia		416		15.38%
Spain		10,741		30.73%
Sweden		1,857		23.36%
Iceland		198		66.67%
Liechtenstein		25		0.00%
Norway		1,225		22.41%
Total EU		76,094		29.93%
Total EEA		77,542		29.92%

Measure 21.2	
QRE 21.2.1	We have undertaken consultations with researchers from the Massachusetts Institute of Technology (US) and the University of Regina (Canada) in order to understand the effect of showing users accurate information after they interacted with a misinformation claim.

	<p>We are exploring ways in which we can leverage this research to consider how we engage with users who have interacted with harmful misinformation on our platform and direct them to authoritative information.</p>
<p>Measure 21.3</p>	
<p>QRE 21.3.1</p>	<p>As set out within our response to QRE 17.1.1, we apply our unverified content and state-controlled media labels to certain content in order to empower our community by providing them with an additional layer of context. We ensure these labels are developed and deployed in line with scientific evidence by partnering with fact-checkers and working with external experts, including scientists, in the following ways:</p> <ul style="list-style-type: none"> <p>Unverified content label. As mentioned above, we partner with a number of IFCN registered fact checkers in Europe, who assist with assessing the accuracy of certain content on our platform. Where our fact-checking partners determine that a video is not able to be confirmed or their fact-checks are inconclusive (which is sometimes the case, particularly during unfolding events or crises), we may apply our unverified content label to the video.</p> <p>We also partnered with behavioural scientists, Irrational Labs, in relation to the roll out of the specialised prompts which encourage users to consider content which has been labelled as unverified, before sharing it. The prompts, which are explained in further detail at QRE 17.1.1, were designed and tested with Irrational Labs. On testing the prompts, Irrational Labs found that viewers decreased the rate at which they shared videos by 24%, while likes on such unsubstantiated content also decreased by 7%.</p> <p>State-controlled media label. In the last year, we have started applying our state-controlled media label to accounts or content belonging to media organisations whose editorial decision making is directly or indirectly controlled by a government. To inform our definition of state-affiliated media and approach to making such designations, we engaged with over 50 experts across 20 countries and will continue to work with these experts to inform our global approach and expansion of the policy.</p> <p>As mentioned above, one of the experts we worked closely with was Irrational Labs. In collaboration with the behavioural scientists, we considered the ways in which we could present the label to our users. As part of this, we tested various copy options across English, Spanish, and Arabic via quantitative surveys and qualitative panels, and found that "[country] state-controlled media" was the option most preferred by users while being</p>

	<p>the most accurate representation of the relevant media entities' relationship to their respective governments.</p> <p>We are also continuously taking user feedback into consideration in order to identify new topics and consider which tools may be best suited to raising awareness around that topic and combating harmful misinformation.</p>
--	--

V. Empowering Users	
Commitment 22	
Relevant Signatories commit to provide users with tools to help them make more informed decisions when they encounter online information that may be false or misleading, and to facilitate user access to tools and information to assess the trustworthiness of information sources, such as indicators of trustworthiness for informed online navigation, particularly relating to societal issues or debates of general interest.	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No
If yes, list these implementation measures here [short bullet points].	TikTok did not subscribe to this commitment.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Aiming to build products and processes to more quickly launch user education interventions when a new crisis emerges.

Measure 22.1	
QRE 22.1.1	<p>Not committed. TikTok considers that the implementation of the other commitments under the Code (including, but not limited to, the other commitments relating to empowering users and fact-checking) provide a comprehensive approach to tackling disinformation, including facilitating users in making more informed decisions when they encounter online information that may be false or misleading. This position is also reflected in the Commission's guidance. As such, TikTok does not consider that committing to this measure will materially add to the other measures being adopted under the Code.</p> <p>TikTok does, however, keep an open mind. As such, it is prepared to explore such solutions with the relevant providers in due course and to reassess whether such an approach would be beneficial, taking into account existing measures in place.</p>
SLI 22.1.1 - actions enforcing policies above	N/A
	N/A
Member States	
Austria	
Belgium	
Bulgaria	
Croatia	
Cyprus	
Czech Republic	
Denmark	
Estonia	
Finland	

France	
Germany	
Greece	
Hungary	
Ireland	
Italy	
Latvia	
Lithuania	
Luxembourg	
Malta	
Netherlands	
Poland	
Portugal	
Romania	
Slovakia	
Slovenia	
Spain	
Sweden	
Iceland	
Liechtenstein	

Norway	
Total EU	
Total EEA	

Measure 22.2	
QRE 22.2.1	Not committed. TikTok does not consider this to be a practical or implementable proposal. In any event, this measure is unnecessary as the combination of other commitments underpinning the Code (including, but not limited to, those relating to fact-checking) represent a comprehensive approach to achieving the goal of providing users with tools to make more informed decisions when they encounter online information that may be false or misleading.
Measure 22.3	
QRE 22.3.1	Not committed. Not relevant, linked to the above Measures.
Measure 22.4	
QRE 22.4.1	Not committed. Measures 22.4, 22.5 and 22.6 are not applicable as TikTok is not a provider of trustworthiness indicators.
SLI 22.4.1 - actions enforcing policies above	N/A
	N/A
Data	Not committed. TikTok does not consider this to be a practical or implementable proposal. In any event, this measure is unnecessary as the combination of other commitments underpinning the Code (including, but not limited to, those relating to fact-checking) represent a comprehensive approach to achieving the goal of providing users with tools to make more informed decisions when they encounter online information that may be false or misleading.

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

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

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

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

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

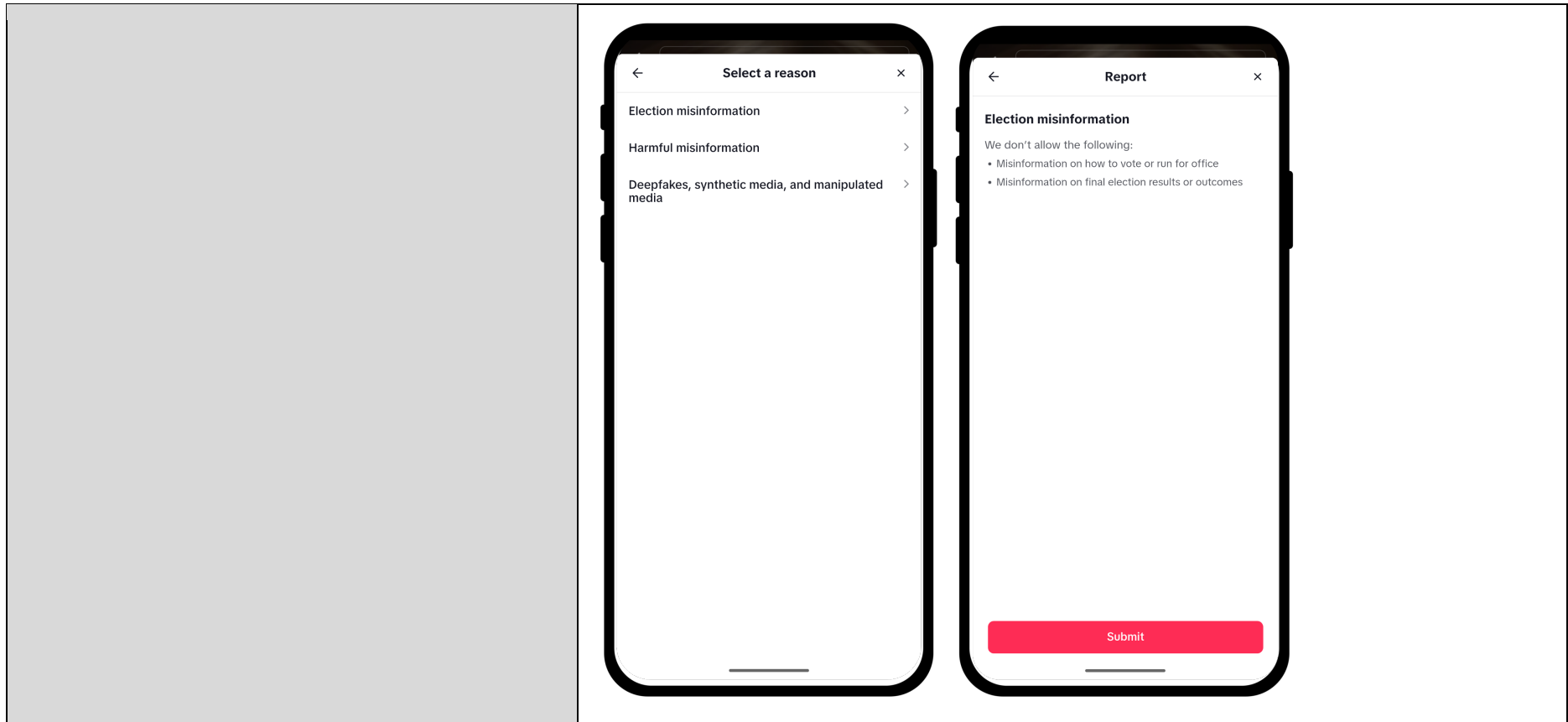
V. Empowering Users

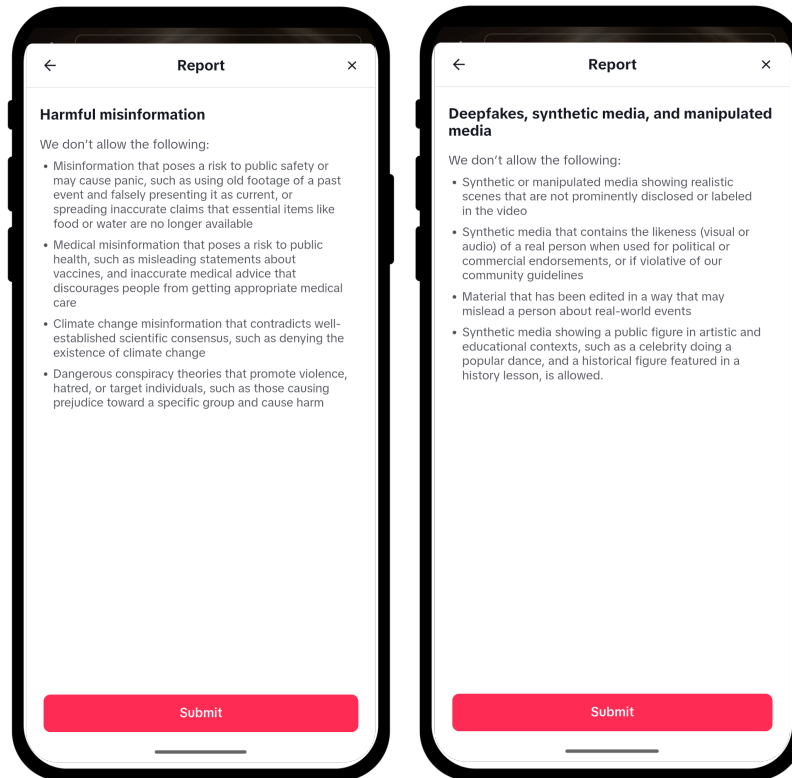
Commitment 23

Relevant Signatories commit to provide users with the functionality to flag harmful false and/or misleading information that violates Signatories policies or terms of service.

<p>In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]</p>	<p>Yes</p>
<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> ● As part of refreshing our CGs, updated our in-app reporting functionality to allow users to report harmful misinformation at a more granular level. ● Implemented a dedicated reporting channels to enable users to report suspected illegal content in line with our DSA requirements and provided a help centre article to improve user transparency on how to do so (here) ● Undertaken work to improve user transparency in relation to our appeals and reporting processes and provided a help centre article to improve user transparency on how to do so (here) ● Continued investing in resources and training for our misinformation moderators and expanded our specialist misinformation moderation teams in the nine countries in which we have added secured fact-checking partnerships.
<p>Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> ● Continued expansion of our fact-checking network, consisting of committing to onboarding new European-based fact-checking partners and increasing our operational coverage in the EEA. As part of these plans, we will be expanding our misinformation moderation teams.

Measure 23.1	
QRE 23.1.1	<p>We provide users with simple, intuitive ways to report/flag content in-app for any breach of our Terms of Service or CGs including for harmful misinformation in each EU member state and in an official language of the European Union.</p> <ul style="list-style-type: none"> • By 'long-pressing' (e.g., clicking for 3 seconds) on the video content and selecting the "Report" option. • By selecting the "Share" button available on the right-hand side of the video content and then selecting the "Report" option. <p>The user is then shown categories of reporting reasons from which to select (which align with the harms our CGs seek to address). We recently updated this feature to make the "Misinformation" categories more intuitive and allow users to report with increased granularity. We have also made changes to implement an additional option to enable users to report illegal content in line with our requirements under DSA.</p>





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

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

Measure 23.2	
QRE 23.2.1	<p><u>Appeals system</u></p> <p>We are transparent with users in relation to appeals and set out (here) the options which may be available where users are not satisfied with decisions we have taken as to whether content is violative, whether that user is the creator of the affected content or the user who reported the content.</p> <p>The integrity of our appeals systems is predominantly ensured through the involvement of our specialised human moderators, who are able to take context into account when reaching decisions in relation to whether content is illegal or incompatible with our CGs and is therefore safe to be shared on our platform.</p> <p>Our moderators review all appeals raised in relation to removed videos, removed comments and banned accounts. In order to reach a decision as to whether the user's content can be reinstated on our platform, our moderators consider whether such content is in violation of our policies. To ensure consistency within this process and its overall integrity, we have sought to make our policies as clear and comprehensive as possible and have put in place robust Quality Assurance processes (including steps such as auditing appeals and undertaking Root Cause Analyses).</p> <p>If users who have submitted an appeal are still not satisfied with our decision, they can share feedback with us via the webform which is available in our Support Centre. We are continuously taking user feedback into consideration in order to identify areas of improvement, including within the appeals process. Users may also have other legal rights in relation to decisions we make, as set out further here.</p> <p><u>Reporting system</u></p> <p>In order to ensure the integrity of our reporting systems, we deploy a combination of automated moderation technology and specifically trained moderators.</p> <p>When a user reports content on our platform, our automated systems will first consider whether it is in violation of our CGs. If a potential violation of our CGs is found, the automated moderation system will either pass it on to our moderation teams for further review or, if there is a high degree of confidence that the content violates our CGs, remove it automatically. Automated removal is only applied when violations are clear-cut, such as where the content contains nudity or youth safety. We are constantly investing in improving the precision of our automated</p>

	<p>moderation systems so we can more effectively remove violative content at scale while also reducing the number of incorrect removals.</p> <p>Where violations are less clear-cut, content will be passed on to our moderation teams for further review, in order to support the fair and consistent review of potentially violative content. As mentioned above, our moderators can take into account additional context and nuance which may not always be picked up by technology. In order to ensure consistency within this process and its overall integrity, we have sought to make our CGs as clear and comprehensive as possible and have put in place robust Quality Assurance processes (including steps such as review of moderation cases, flows, appeals and undertaking Root Cause Analyses).</p> <p>In order to meet our requirements set out under the DSA, we have introduced a dedicated reporting channel for users to report suspected illegal content. When a user reports suspected illegal content, we will first review the content to assess whether it violates our CGs. However, if we do not determine that the content violates our CGs and sufficient information has been provided in the report, we have a dedicated moderation team which will check whether the content is illegal.</p> <p>We also note that whilst user reports are important, at TikTok we place considerable emphasis on proactive content moderation and so are proud that the vast majority of content is identified and removed proactively before it receives any views or is reported to us.</p>
--	---

V. Empowering Users	
Commitment 24	
<p>Relevant Signatories commit to inform users whose content or accounts has been subject to enforcement actions (content/accounts labelled, demoted or otherwise enforced on) taken on the basis of violation of policies relevant to this section (as outlined in Measure 18.2), and provide them with the possibility to appeal against the enforcement action at issue and to handle complaints in a timely, diligent, transparent, and objective manner and to reverse the action without undue delay where the complaint is deemed to be founded.</p>	
<p>In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]</p>	<p>Yes</p>

<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> ● Improved the user notification received following action on a user's account or content to include further granularity on the action taken and a simple way to appeal the decision taken. ● Improved user transparency around our appeals processes (here)
<p>Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> ● Continuing to review our user notification and appeal process and consider any feedback received from users and stakeholders on its user
<p>Measure 24.1</p>	
<p>QRE 24.1.1</p>	<p>Users in all EU member states are notified by an in-app notification in their relevant local language where the following action is taken:</p> <ul style="list-style-type: none"> ● removal or otherwise restriction of access to their content; ● A ban of the account; ● restriction of their access to a feature (such as LIVE); or ● restriction of their ability to monetise. <p>Such notifications are provided in near real time after action has been taken (i.e. generally within several seconds or up to a few minutes at most).</p> <p>Where we have taken any of these decisions, an in-app inbox notification sets out the violation deemed to have taken place, along with an option for users to “disagree” and submit an appeal. Users are able to submit appeals within 180 days of being notified of the decision they want to appeal. Further information, including about how to appeal a report is set out here.</p> <p>All such appeals raised will be queued for review by our specialised human moderators so as to ensure that context is adequately taken into account in reaching a determination. Users can monitor the status and view the results of their appeal within their in-app inbox.</p>

	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.			
SLI 24.1.1 - enforcement actions	Methodology of data measurement:			
	<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 harmful misinformation policies.</p> <p>The appeal success rate of videos removed by our harmful misinformation policies is based on the ratio between the number of appeals raised and the number of successful appeals (i.e. overturns).</p>			
	Nr of enforcement actions	Nr of actions appealed	Metrics on results of appeals	Metrics on the duration and effectiveness of the appeal process
Member States				
List actions per member states and languages (see example table above)	Number of accounts removed banned under our I&A policies	Number of appeals of videos removed for violation of harmful misinformation policy	Number of successful appeals for violation of harmful misinformation policy (i.e. overturns)	Appeal success rate of videos removed for violation of harmful misinformation policy
Member States				
Austria	67	273	44	16.12%
Belgium	155	534	296	55.43%

Bulgaria	121	74	31	41.89%
Croatia	28	23	17	73.91%
Cyprus	6	71	15	21.13%
Czech Republic	59	409	227	55.50%
Denmark	62	115	37	32.17%
Estonia	8	2	1	50.00%
Finland	55	115	68	59.13%
France	1,106	8,328	3,506	42.10%
Germany	1,272	5,295	927	17.51%
Greece	73	260	72	27.69%
Hungary	35	162	104	64.20%
Ireland	144	644	377	58.54%
Italy	910	12,865	3,778	29.37%
Latvia	9	10	7	70.00%
Lithuania	19	9	8	88.89%
Luxembourg	2	2	1	50.00%
Malta	4	1	1	100.00%

Netherlands	802	737	339	46.00%
Poland	731	1,579	827	52.37%
Portugal	63	115	60	52.17%
Romania	373	879	543	61.77%
Slovakia	28	189	94	49.74%
Slovenia	17	8	4	50.00%
Spain	432	4,344	2,316	53.31%
Sweden	266	768	359	46.74%
Iceland	26	5	5	100.00%
Liechtenstein	0	0	0	0.00%
Norway	296	614	90	14.66%
Total EU	6,847	37,811	14,059	37.18%
Total EEA	7,169	38,430	14,154	36.83%

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]	No
If yes, list these implementation measures here [short bullet points].	This commitment is not applicable as TikTok is not a messaging app.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No
If yes, which further implementation measures do you plan to put in place in the next 6 months?	This commitment is not applicable as TikTok is not a messaging app.
Measure 25.1	
QRE 25.1.1	Not committed. This commitment is not applicable as TikTok is not a messaging app.
SLI 25.1.1	N/A
	N/A

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

VI. Empowering the research community
Commitments 26 - 29

VI. Empowering the research community

Commitment 26

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

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	<ul style="list-style-type: none"> • Worked on expanding our Research API to Europe which provides researchers with access to public data on content and accounts from our platform. • Launched the Commercial Content API in Europe to bring transparency to paid advertising and other content that's commercial in nature on TikTok
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	<ul style="list-style-type: none"> • Launching the expansion of the Research API to Europe and EU-based researchers. • Continuing to seek feedback from researchers on their use of the Research API and Commercial Content API and to make updates to better support independent research and transparency into TikTok.
Measure 26.1	
QRE 26.1.1	We have a dedicated TikTok Transparency Centre available in a number of EU languages which hosts:

	<ul style="list-style-type: none"> • Our six-monthly Code reports, outlining our measures for combatting disinformation on our platform and disclosing approximately 2,500 metrics relating to disinformation. • Our TikTok Community Guideline Enforcement Reports, outlining the action we take against content and accounts that violate any of our CGs on a quarterly basis. <p>We also have a dedicated TikTok for Developers website which hosts our Research and Commercial Content APIs (detailed below).</p>			
<p>QRE 26.1.2</p>	<p>TikTok is committed to continue to publish approximately 2,500 metrics relating to disinformation in our six-monthly Code reports. In our January 2023 Code report, TikTok disclosed the most detailed data compared to other Code signatories in terms of breadth (for the entire Q4 2022 period) and depth of reporting (across 30 EEA member states). We are pleased to confirm that for this latest reporting period that we have worked hard to largely address any outstanding data gaps and further increased transparency in certain areas by disclosing new metrics.</p> <p>We also provide transparency on the action we take against content and accounts that violate any of our CGs on a quarterly basis in our TikTok Community Guideline Enforcement Reports. We provide accessible graphs showcasing key metrics, as well as access to aggregated data in a downloadable form. We work hard to supplement the comprehensive data we already provide and provide new insights. By way of example, we recently shared data on our response time to remove violative content reported by our community using our in-app and online reporting tools.</p> <p>We provide access to researchers to data that is publicly available on our platform through our Research API and relating to commercial content through our Commercial Content API (detailed below).</p>			
<p>SLI 26.1.1 - uptake of the tools and processes described in Measure 26.1</p>	<table border="1" style="width: 100%; height: 100%;"> <tr> <td style="width: 33%;"></td> <td style="width: 33%;"></td> <td style="width: 33%;"></td> </tr> </table>			
<p>Data</p>	<table border="1" style="width: 100%; height: 100%;"> <tr> <td style="width: 60%;"></td> <td style="width: 40%;"></td> </tr> </table>			
<p>Measure 26.2</p>	<table border="1" style="width: 100%; height: 100%;"> <tr> <td style="width: 100%;"></td> </tr> </table>			
<p>QRE 26.2.1</p>	<p>(I) Research API</p>			

	<p>We are pleased to have built a Research API that provides researchers with access to public data on content, accounts and comments from our platform. More information is available here. It was initially launched in the US and accessed by US-based academic researchers and it has been expanded to the EEA, UK and Switzerland. We have carefully considered feedback shared with us by researchers who have used the API to date, and on the basis of this feedback, we have already made improvements including streamlining the application process and enabling Lab Access, which will give research project teams in the same university more flexibility to provide access for up to 10 researchers</p> <p>(II) Commercial Content API</p> <p>As part of our requirements under the DSA, we have built commercial content related APIs that includes ads, ad and advertiser metadata, 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>						
<p>QRE 26.2.2</p>	<p>See our response to QRE 26.1.1.</p>						
<p>QRE 26.2.3</p>	<p>For both our Research API and Commercial Content API, we make detailed information available to researchers on what data is made available and how researchers can apply for access. We provide step-by-step instructions for researchers on how to access research data once their application has been approved including how to comply with the security steps and how to run queries on the data. This information is provided on a dedicated website called TikTok for Developers.</p>						
<p>SLI 26.2.1 - meaningful metrics on the uptake, swiftness, and acceptance level of the tools and processes in Measure 26.2</p>	<p>Since launching the TikTok Research API, we've had more than 60 applications from US non-profit academic researchers on topics related to consumer trends, misinformation, mental health and more. We are committed to sharing metrics in the next reporting period on its use by EU-based researchers.</p> <table border="1" data-bbox="869 1310 2042 1375"> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </table>						

Data						
Measure 26.3						
QRE 26.3.1	<p>We welcome feedback from researchers on our APIs and have provided a dedicated contact point to facilitate receiving their feedback. We have carefully considered feedback shared with us by US-based researchers who have accessed the Research API, and on the basis of this feedback, we have already made improvements prior to the API's expansion to Europe including streamlining the application process and enabling Lab Access.</p>					

VI. Empowering the research community	
Commitment 27	
<p>Relevant Signatories commit to provide vetted researchers with access to data necessary to undertake research on Disinformation by developing, funding, and cooperating with an independent, third-party body that can vet researchers and research proposals.</p>	
<p>In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]</p>	<p>Yes</p>
<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> ● Committed to participating in a data access pilot with EDMO in order to trial the process for sharing data with vetted researchers as designated under the DSA. ● Participated in the working group which has been set up to implement the independent third party body. ● Contributed to the European Commission's Call for Evidence on Data Access under the DSA.
<p>Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]</p>	<p>Yes</p>

<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> • Continue participating in the working group which has been set up to implement the independent third party body. • Progressing our work on the EDMO data access, which explores data sharing with vetted researchers designated under the DSA, and actively collaborating with EDMO on a regular basis to progress this.
<p>Measure 27.1</p>	
<p>QRE 27.1.1</p>	<p>We have been engaging with EDMO as part of this process and are participating in the working group that has been set up in order to implement the independent third party body that is referred to above.</p> <p>TikTok also contributed to the European Commission's Call for Evidence on Data Access under the DSA. We submitted a comprehensive response reflecting feedback from cross-functional teams within TikTok from data scientists to privacy experts.</p> <p>TikTok has committed to participate in a data access pilot with EDMO in order to trial the process for sharing data with vetted researchers designated under the DSA. We are one of the few platforms that have committed the resources and time to partake in the pilot. The pilot is aimed at informing the future processes around granting access to data under this Code and Article 40(4), DSA.</p>
<p>Measure 27.2</p>	
<p>QRE 27.2.1</p>	<p>We are participating in the working group which has been set up to implement the independent third party body.</p>
<p>Measure 27.3</p>	
<p>QRE 27.3.1</p>	<p>We are participating in the working group which has been set up to implement the independent third party body. TikTok has committed to participate in a data access pilot with EDMO in order to trial the process for sharing data with vetted researchers designated under the DSA.</p>
<p></p>	<p>N/A</p>

SLI 27.3.1 - research projects vetted by the independent third-party body	N/A
Data	
Measure 27.4	
QRE 27.4.1	We have committed to participate in a data access pilot with EDMO in order to trial the process for sharing data with vetted researchers designated under the DSA. We are one of the few platforms that have committed the resources and time to partake in the pilot. The pilot is aimed at informing the future processes around granting access to data under this Code and Article 40(4), DSA.

VI. Empowering the research community	
Commitment 28	
Relevant Signatories commit to support good faith research into Disinformation that involves their services.	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	<ul style="list-style-type: none"> • Worked on expanding our Research API to Europe which provides researchers with access to public data on content and accounts from our platform. • Launched the Commercial Content API in Europe to bring transparency to paid advertising and other content that's commercial in nature on TikTok • Committed to participating in a data access pilot with EDMO in order to trial the process for sharing data with vetted researchers as designated under the DSA.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the	Yes

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?	<ul style="list-style-type: none"> ● Launching the expansion of the Research API to Europe and EU-based researchers. ● Continuing to seek feedback from researchers on their use of the Research API and Commercial Content API and to make updates to better support independent research and transparency into TikTok. ● Progressing our work on the EDMO data access, which explores data sharing with vetted researchers designated under the DSA, and actively collaborating with EDMO on a regular basis to progress this.
Measure 28.1	
QRE 28.1.1	<p>TikTok is committed to facilitating research and engaging with the research community.</p> <p>We have in place a Safety Advisory Council for Europe that brings together independent leaders from academia and civil society from all around the continent. Each member provides subject matter expertise as they advise on issues relating to users safety, content policies and areas of social relevance.</p> <p>In addition, many of our teams engage with the research community.</p> <p>Our Outreach & Partnerships Management Team is dedicated to engaging regularly with, and setting up partnerships with, the academic and research community. This team, together with our subject matter experts within our product team, are central to our fact-checking programme from identifying new partners and onboarding them to regularly meeting with them.</p> <p>More generally, our Trust and Safety teams regularly consult and engage with the research community, including on harmful misinformation and deceptive behaviours, when updating or launching new policies or features on our platform.</p> <p>For instance, our teams have engaged with dozens of academics in Europe as part of the development and implementation of our policy related to state affiliated media.</p>

	<p>During election times, we also consult expert partners to provide us with insights to better understand areas that could potentially amount to election manipulation.</p> <p>We also have many teams committing time to facilitating research. Individuals with backgrounds in product, data science, outreach and legal are working together to develop and roll-out our APIs (as outlined above).</p> <p>TikTok representatives also regularly participate in research-focused events. Relevant examples include the Terrorism and Social Media Conference (Swansea University), the Trust and Safety Research Conference (Stanford University), and the Association of Internet Researchers Conference (Technological University Dublin). At these events we seek to learn from the important work being done by the research community on various topics, which include aspects related to harmful misinformation, as well as share context about our approach, research interests, and opportunities to collaborate.</p>
Measure 28.2	
QRE 28.2.1	<p>We have a dedicated TikTok for Developers website which hosts APIs for our research information.</p> <p>With the Research API, researchers can access:</p> <ul style="list-style-type: none"> ● Public account data, such as user profiles, comments, performance data, such as number of comments, likes, and favorites that the user receives ● Public content data, such as comments, captions, subtitles, performance data, such as number of comments, shares, likes, and favorites that the video receives ● Public data for keywords search results <p>Our commercial content related APIs includes ads, ad and advertiser metadata, 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	We are eager to engage and cooperate with EDMO as part of this annual consultation and to receive feedback from the research community on how we facilitate their research projects on our platform.
Measure 28.4	
QRE 28.4.1	We are committed to collaborating with EDMO and regularly engage with EDMO including on a pilot to share data with vetted researchers as designated by the DSA.

VI. Empowering the research community	
Commitment 29	
Relevant Signatories commit to conduct research based on transparent methodology and ethical standards, as well as to share datasets, research findings and methodologies with relevant audiences.	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No
If yes, list these implementation measures here [short bullet points].	This Commitment relates to Research Organisations.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No

If yes, which further implementation measures do you plan to put in place in the next 6 months?	This Commitment relates to Research Organisations.
Measure 29.1	
QRE 29.1.1	Not committed.
QRE 29.1.2	Not committed.
QRE 29.1.3	Not committed.
SLI 29.1.1 - reach of stakeholders or citizens informed about the outcome of research projects	N/A
	N/A
Data	
Measure 29.2	Not committed.
QRE 29.2.1	Not committed.
QRE 29.2.2	Not committed.
QRE 29.2.3	N/A
SLI 29.2.1	N/A
	Not committed.
Data	

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

VII. Empowering the fact-checking community
Commitments 30 - 33

VII. Empowering the fact-checking community

Commitment 30

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

<p>In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]</p>	<p>Yes</p>
<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> ● Continued to progress the rapid scale-up of our fact-checking program and exceeded our commitment to expand our fact-checking to four EU countries. Instead, we launched dedicated fact-checking programs in nine new EEA countries (Denmark, Finland, Norway, Greece, Cyprus, Belgium, Czech Republic, Slovakia, and Bulgaria) and expanded our misinformation moderation teams for those languages. ● Sponsored and presented at a fact-checking summit (GlobalFact 10), which was hosted by the IFCN and widely attended by stakeholders from the international fact-checking community. ● Continued to develop our internal repository of previously fact-checked claims to help our specialised misinformation moderators make swift and accurate decisions. ● Revamped our agreements with our fact-checking partners in order to reflect feedback from our partners and build in further flexibility to collaborate with partners on new projects or expand scope where needed. ● Increased our ability to receive pro-active flagging of potential misinformation from our fact-checking partners. ● Implemented our pilot scheme to share enforcement data with our fact-checking partners on the claims they have provided feedback on. ● Continued to conduct regular surveys with our partners to review our working relationship. ● Continued to regularly participate in the fact-checking working group.
<p>Do you plan to put further implementation measures in place in the next 6 months to substantially improve the</p>	<p>Yes</p>

<p>maturity of the implementation of this commitment? [Yes/No]</p>	
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<ul style="list-style-type: none"> ● Continued expansion of our fact-checking network, consisting of committing to on-boarding new European-based fact-checking partners and increasing our operational coverage in the EEA. As part of these plans, we will be expanding our misinformation moderation teams. ● Continuing to develop our fact-checking repository, as well as continuing to participate in the sub-group on the creation of an external repository. ● Further increasing the quality of our method of data sharing with fact-checking partners.
<p>Measure 30.1</p>	
<p>QRE 30.1.1</p>	<p>Within Europe, we work with 9 fact-checking partners who provide fact-checking coverage in 17 official EU languages. Our partners have teams of fact-checkers who review and verify reported content. Our moderators then use that independent feedback to take action and where appropriate, remove or make ineligible for recommendation false or misleading content or label unverified content.</p> <p>Our agreements with our partners are standardised, meaning the agreements are based on our template master services agreements and consistent 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. ● The expected results e.g., the fact-checkers advise on whether the content may be or contain misinformation and rate it using our classification categories. ● An option to agree that our fact-checker partners provide regular written reports about disinformation trends identified. ● The languages in which they will provide fact-checking services. ● The ability to request temporary coverage regarding additional languages if needed. ● All other key terms including the applicable term and fees and payment arrangements.

	<p>We used the opportunity of the annual review process to agree to revamped agreements with our fact-checking partners. The new agreements reflected feedback from our partners and built in further flexibility to facilitate our partners debunking an expanded type of claims in further languages or supporting on ad hoc additional projects. We have also increased our ability to receive pro-actively flagging of potential misinformation from our fact-checking partners.</p>
<p>QRE 30.1.2</p>	<p>Within Europe, our IFCN-accredited fact-checking partners are:</p> <ol style="list-style-type: none"> 1. Agence France Press; 2. Facta.news; 3. Lead Stories; 4. Logically; 5. Newtral; 6. Science Feedback; 7. dpa Deutsche Presse-Agentur 8. Teyit; and 9. Reuters <p>We can, and have, put in place temporary agreements with these fact checking partners to provide additional European language coverage for a period in an unfolding crisis.</p> <p>Outside of our fact-checking program, we also collaborate with a variety of fact-checking partners to develop media literacy campaigns and work on other discrete projects. For example, we have previously collaborated with Fakenews.pl, Maldita and Correctiv on media literacy campaigns.</p> <p>Globally, we have 15 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 17 official European languages (Dutch, English, French, German, Hungarian, Italian, Polish, Romanian, Spanish, Swedish, Danish, Finnish, Norwegian, Greek, Czech, Slovakian, and Bulgarian), and, therefore, the spoken language of 22 EEA countries.</p> <p>We can request additional support in relation to a number of European languages or languages which affect European users, including Azeri, Armenian, Turkish, Russian, Ukrainian and Belarusian.</p>

In terms of global fact-checking initiatives, we currently cover more than 50 languages and assess content in more than 100 countries, thereby improving the overall integrity of the service and benefiting European users. As mentioned, we are progressing our ambitious plans to continue the expansion of our fact-checking network in Europe and globally.

In order to effectively scale the feedback provided by our fact-checkers globally, we have implemented the measures listed below.

- **Fact-checking repository.** We have built a database of claims which have previously been fact-checked by our EU and global fact checking partners.
- **Trends reports.** Our fact-checking partners can provide us with regular reports identifying general misinformation trends observed on our platform and across the industry generally, including new/changing industry or market trends, events or topics that generated particular misinformation or disinformation.
- **Proactive detection by our fact-checking partners.** Our fact-checking partners are authorised to proactively identify content that may constitute harmful misinformation on our platform and suggest prominent misinformation that is circulating on other social media platforms or websites that may benefit from verification. We have utilised the opportunity of the recent revamp of our agreements with our fact-checking partners to increase our ability to receive pro-active flagging of potential misinformation from our partners.
- **Fact-checking guidelines.** We create guidelines and trending topic reminders for our moderators on the basis of previous fact-checking assessments. This ensures our moderation teams leverage the insights from our fact-checking partners and helps our moderators make swift and accurate decisions on flagged content regardless of the language in which the original claim was made.

Our specialised misinformation moderation teams have direct access to these tools and measures, which enables them to more swiftly, easily and accurately take action on violating content across Europe and globally.

We are continuing to invest in building, and improving, models which may allow for the output of these measures to be used to update the machine learning models we use in proactive detection, learning, over time, to search for similar content which can be proactively recalled into our moderation system for review. Leveraging the fact-checking output in this way would enable us to further increase the positive impact of our fact checking programme.

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

Ireland	Fact-checking coverage implemented
Italy	Fact-checking coverage implemented
Latvia	We are working hard to continue to expand our fact-checking programme. Meanwhile, our fact-checking repository and other initiatives benefit all European users and ensure the overall integrity of our platform.
Lithuania	
Luxembourg	Fact-checking coverage implemented
Malta	We are working hard to continue to expand our fact-checking programme. Meanwhile, our fact-checking repository and other initiatives benefit all European users and ensure the overall integrity of our platform.
Netherlands	
Poland	Fact-checking coverage implemented
Portugal	We are working hard to continue to expand our fact-checking programme. Meanwhile, our fact-checking repository and other initiatives benefit all European users and ensure the overall integrity of our platform.
Romania	Fact-checking coverage implemented
Slovakia	Fact-checking coverage implemented
Slovenia	We are working hard to continue to expand our fact-checking programme. Meanwhile, our fact-checking repository and other initiatives benefit all European users and ensure the overall integrity of our platform.
Spain	Fact-checking coverage implemented
Sweden	Fact-checking coverage implemented

Iceland	We are working hard to continue to expand our fact-checking programme. Meanwhile, our fact-checking repository and other initiatives benefit all European users and ensure the overall integrity of our platform.
Liechtenstein	Fact-checking coverage implemented
Norway	Fact-checking coverage implemented
Total EU	20
Total EEA	22

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. We reviewed and updated our standard agreements in time for our 2023 annual contract renewal process to ensure consistency across all our global partners.</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>

	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.
QRE 30.2.2	<p>We meet regularly with our fact-checking partners and have an ongoing dialogue with them about how our partnership is working and evolving. We survey our fact-checking partners to encourage feedback about what we are doing well and how we could improve.</p> <p>We have recently initiated a pilot scheme to share fact-checking enforcement data with our fact-checking partners which has been well received. Impact assessments are currently shared on a bimonthly basis. Going forward, we plan to further increase the quality of our methods of data sharing with fact-checking partners.</p>
QRE 30.2.3	This provision is not relevant to TikTok, only to fact-checking organisations.
Measure 30.3	
QRE 30.3.1	Given our fact-checking partners are all IFCN-accredited, our fact-checking partners already engage in some informal cross-border collaboration through that network. In addition, we continue to collaborate with our partners to understand how we may be able to facilitate further collaboration. A recent example is prior to the Turkish election in May 2023, we facilitated a pilot collaboration project between our German fact-checking partner, dpa Deutsche Presse-Agentur, and our Turkish fact-checking partner, Teyit, seeking to process Turkish election content in German. We established a communication channel to allow for information sharing between our two partners.
Measure 30.4	
QRE 30.4.1	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.

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].

- Expanded our fact-checking coverage to 9 further EEA countries (Denmark, Finland, Norway, Greece, Cyprus, Belgium, Czech Republic, Slovakia, and Bulgaria), and in parallel, expanded our misinformation moderation teams for those languages.
- Continued to expand our fact-checking repository to ensure our teams and systems leverage the full scope of insights our fact-checking partners submitted to TikTok (regardless of the original language of the relevant content).
- Participated in the newly created working group within the Code framework on the creation of an external fact-checking repository.

Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]

Yes

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

- Continued expansion of our fact-checking network, consisting of committing to onboarding new European-based fact-checking partners and increasing our operational coverage in the EEA (and expanding our misinformation moderation teams in parallel).
- Continuing to develop our fact-checking repository and tools for fact-checking repository.
- Continue to work with the relevant working group to create an external repository of fact-checking content.

Measure 31.1	
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 9 fact-checking partners in Europe, covering 17 official European languages.</p> <p>While we use machine learning models to help detect potential misinformation, our approach is to have our specialised misinformation moderators 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>Out of an abundance of caution, while content is being fact-checked or when content can't be substantiated through fact-checking, we may significantly reduce the content's distribution so that fewer people see it. Fact-checkers ultimately do not take action on the content directly. The moderator will instead take into account the fact-checkers' feedback on the accuracy of the content when deciding whether the content violates our CGs and what action to take.</p> <p>(ii) contributing to our global database of previously fact-checked claims to help our misinformation moderators make swift and accurate 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 sometimes 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</p>

	<p>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> <p>As we have substantially expanded our fact-checking network and the period upon which we are reporting, there has been a corresponding increase in the volume of fact checked content we are able to report on. We are also working internally to develop metrics which meaningfully demonstrate the impact of our fact-checking programme across Europe.</p>			
SLI 31.1.1 - use of fact-checks	Methodology of data measurement:			
	The number of fact checked videos is based on the number of videos that have been sent for review to one of our fact-checking partners in the relevant territory.			
	Nr of fact-checked articles published			
List actions per member states and languages (see example table above)	Number of fact checked videos (tasks)			
Member States				
Austria	17			
Belgium	268			
Bulgaria	6			
Croatia	0			
Cyprus	39			
Czech Republic	12			
Denmark	43			
Estonia	3			
Finland	65			

France	2,698			
Germany	477			
Greece	89			
Hungary	6			
Ireland	155			
Italy	1,109			
Latvia	0			
Lithuania	2			
Luxembourg	0			
Malta	0			
Netherlands	114			
Poland	18			
Portugal	60			
Romania	3,385			
Slovakia	13			
Slovenia	0			
Spain	933			
Sweden	669			
Iceland	0			
Liechtenstein	1			

Norway	341			
Total EU	10,181			
Total EEA	10,523			

SLI 31.1.2 - impact of actions taken	Methodology of data measurement:		
	<p>The number of videos removed as a result of a fact checking assessment and the number of videos removed because of policy guidelines, known misinformation trends and our knowledge based repository is based on the country in which the video was posted.</p> <p>These metrics correspond to the numbers of removals under the harmful misinformation policy since all of its enforcement are based on the policy guidelines, known misinformation trends and knowledge based repository.</p>		
	N/A		
List actions per member states and languages (see example table above)	Number of videos removed as a result of a fact checking assessment	Number of videos removed because of policy guidelines, known misinformation trends and knowledge based repository	
Member States			
Austria	1	1,097	
Belgium	68	2,115	
Bulgaria	0	171	
Croatia	0	52	
Cyprus	4	204	
Czech Republic	0	932	

Denmark	7	466	
Estonia	1	28	
Finland	1	459	
France	797	30,677	
Germany	111	18,747	
Greece	14	1,217	
Hungary	0	437	
Ireland	21	2,165	
Italy	337	45,510	
Latvia	0	18	
Lithuania	0	43	
Luxembourg	0	13	
Malta	0	3	
Netherlands	4	2,624	
Poland	4	4,157	
Portugal	20	448	
Romania	1,087	4,656	
Slovakia	0	402	
Slovenia	0	33	
Spain	185	20,493	

Sweden	186	3,468	
Iceland	0	21	
Liechtenstein	1	0	
Norway	138	2,055	
Total EU	2,848	140,635	
Total EEA	2,987	142,711	

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)	Number of videos removed as a result of a fact checking assessment / number of removals under harmful misinformation policy
Austria	0.09%
Belgium	3.22%
Bulgaria	0.00%
Croatia	0.00%
Cyprus	1.96%

Czech Republic	0.00%
Denmark	1.50%
Estonia	3.57%
Finland	0.22%
France	2.60%
Germany	0.59%
Greece	1.15%
Hungary	0.00%
Ireland	0.97%
Italy	0.74%
Latvia	0.00%
Lithuania	0.00%
Luxembourg	0.00%
Malta	0.00%
Netherlands	0.15%
Poland	0.10%
Portugal	4.46%
Romania	23.35%
Slovakia	0.00%
Slovenia	0.00%

Spain	0.90%
Sweden	5.36%
Iceland	0.00%
Liechtenstein	0.00%
Norway	6.72%
Total EU	2.03%
Total EEA	2.09%

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

VII. Empowering the fact-checking community

Commitment 32

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.

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"> Developed and implemented a pilot scheme to share data on a bimonthly basis with our fact checking partners about how often their assessments result in enforcements on TikTok.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	<ul style="list-style-type: none"> Increasing the quality of our methods of data sharing with fact-checking partners.
Measure 32.1	
Measure 32.2	
QRE 32.1.1	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

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

VII. Empowering the fact-checking community

Commitment 33

Relevant Signatories (i.e. fact-checking organisations) commit to operate on the basis of strict ethical and transparency rules, and to protect their independence.

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	No	
If yes, list these implementation measures here [short bullet points].	This Commitment and Measure relates to fact checking organisations.	
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	No	
If yes, which further implementation measures do you plan to put in place in the next 6 months?	This Commitment and Measure relates to fact checking organisations.	
Measure 33.1		
QRE 33.1.1	Not committed. This Commitment and Measure relates to Fact-Checking organisations.	
SLI 33.1.1 - number of European fact-checkers that are IFCN-certified	N/A	

VIII. Transparency Centre
Commitments 34 - 36

VIII. Transparency Centre

Commitment 34

To ensure transparency and accountability around the implementation of this Code, Relevant Signatories commit to set up and maintain a publicly available common Transparency Centre website

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	We have been an active participant in the working group that has successfully launched the common Transparency Centre this year.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	We are committed to maintaining the common Transparency Centre and to continuing our active participation in the Transparency working group.

Measure 34.1	
Measure 34.2	
Measure 34.3	
Measure 34.4	
Measure 34.5	

VIII. Transparency Centre	
Commitment 35	
Signatories commit to ensure that the Transparency Centre contains all the relevant information related to the implementation of the Code's Commitments and Measures and that this information is presented in an easy-to-understand manner, per service, and is easily searchable.	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	<ul style="list-style-type: none"> • Through our participation in the working group that has successfully launched the common Transparency Centre this year, we have ensured that the Centre will allow the general public to access general information about the Code as well as the underlying reports (and for the Centre to be navigated both by commitment and signatory). • We have supported the working group in collecting feedback on the user experience of the website. We have engaged with the vendor to increase the robustness of the website and make improvements to the interface.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the	Yes

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?	<ul style="list-style-type: none"> ● We are committed to maintaining the common Transparency Centre and to continuing our active participation in the Transparency working group. ● We will continue to seek feedback from relevant stakeholders to better maintain and update the website.
Measure 35.1	
Measure 35.2	
Measure 35.3	
Measure 35.4	
Measure 35.5	
Measure 35.6	

VIII. Transparency Centre

Commitment 36

Signatories commit to updating the relevant information contained in the Transparency Centre in a timely and complete manner.

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	We have supported the working group in collecting feedback on the user experience of the website.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	We are committed to maintaining the common Transparency Centre and, as part of this, updating the requisite information in a timely and complete manner.
Measure 36.1	
Measure 36.2	
Measure 36.3	
QRE 36.1.1 (for the Commitments 34-36)	We are pleased to confirm that we have been an active participant in the working group that has successfully launched the common Transparency Centre this year. We have assisted with establishing the website's requirements, selecting a vendor to build the website and overseeing the development of the website's key functionalities and interface. We have ensured that the

	<p>Centre will allow the general public to access general information about the Code as well as the underlying reports (and for the Centre to be navigated both by commitment and signatory). Each signatory will be responsible for ensuring that the information they upload to the website is correct and accurate. Entities interested in joining the Code's Task-force will be able to sign up through a dedicated online application form on the website. We have supported the working group in collecting feedback on the user experience of the website and will continue to seek such feedback from relevant stakeholders to better maintain and update the website.</p>
QRE 36.1.2 (for the Commitments 34-36)	We are committed to maintaining the website and supporting the development of relevant SLIs.
SLI 36.1.1 - (for Measures 34 and 36) meaningful quantitative information on the usage of the Transparency Centre, such as the average monthly visits of the webpage.	We are working with the vendor to support the development of relevant metrics for this SLI.
Data	The common Transparency Center has been visited by around 8,300 users globally between January 30th 2023 and June 30th 2023. The average engagement time on the website is 1m 22s.

IX. Permanent Task-Force
Commitment 37

IX. Permanent Task-Force

Commitment 37

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

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	We have meaningfully engaged in the Task-force and all of its working groups and subgroups. We have joined new relevant groups when created, such as the Elections working group which TikTok co-chairs and the Generative AI working group which will commence in September.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	We will continue to engage in the Task-force and all of its working groups and subgroups.

Measure 37.1	
Measure 37.2	
Measure 37.3	
Measure 37.4	
Measure 37.5	
Measure 37.6	
QRE 37.6.1	<p>We have meaningfully engaged in the Task-force and all of its working groups and subgroups:</p> <ul style="list-style-type: none"> ● Monitoring and Reporting ● Integrity of Services ● Crisis Response ● Transparency Centre ● Outreach ● Ad Scrutiny ● Fact-checking ● Elections <p>We will continue to engage in the Task-force and all of its working groups and subgroups.</p>

X. Monitoring of Code
Commitment 38 - 44

X. Monitoring of Code

Commitment 38

The Signatories commit to dedicate adequate financial and human resources and put in place appropriate internal processes to ensure the implementation of their commitments under the Code.

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes.
If yes, list these implementation measures here [short bullet points].	<ul style="list-style-type: none"> Globally more than 40,000 Trust and Safety professionals are dedicated to keeping TikTok safe.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	Continue to dedicate resources in line with our ongoing obligations under the Code.
Measure 38.1	
QRE 38.1.1	<p>TikTok has assigned the highest priority level to the Code, which means that we have, and will continue to have, appropriate resources in place to meet our commitments and compliance.</p> <p>Given the breadth of the Code and the commitments therein, our work spans multiple teams, including Trust and Safety, Legal, Monetisation Integrity, Product and Public Policy. Teams across the globe are deployed to ensure that we meet our commitments and compliance with</p>

	<p>the notable involvement of our Trust and Safety Leadership team which is based in Dublin, Ireland.</p> <p>TikTok has thousands of content moderators globally and across the European region, as we recognise the importance of local knowledge and expertise as we work to ensure online safety for our users. We take a similar approach to our third party partnerships.</p>
--	--

X. Monitoring of Code	
<p>Commitment 39</p> <p>Signatories commit to provide to the European Commission, within 1 month after the end of the implementation period (6 months after this Code's signature) the baseline reports as set out in the Preamble.</p>	
In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	We have shared our second report with the Commission in accordance with the agreed timeframes.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	We are committed to continue to report on our Code commitments on a regular basis within the agreed timeframes.

X. Monitoring of Code

Commitment 40

Signatories commit to provide regular reporting on Service Level Indicators (SLIs) and Qualitative Reporting Elements (QREs). The reports and data provided should allow for a thorough assessment of the extent of the implementation of the Code's Commitments and Measures by each Signatory, service and at Member State level.

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	We have reported on the SLIs and QREs relevant to the Commitments we signed-up to within this report at a level of detail beyond any previous transparency efforts.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	We are committed to reporting on the SLIs and QREs relevant to the Commitments we signed-up to in line with the timeframes agreed.

Measure 40.1	
Measure 40.2	
Measure 40.3	
Measure 40.4	
Measure 40.5	
Measure 40.6	

X. Monitoring of Code

Commitment 41

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

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

Yes

<p>If yes, list these implementation measures here [short bullet points].</p>	<ul style="list-style-type: none"> • We have been an active participant in the working group dedicated to developing Structural Indicators. • We supported the publication of pilot Structural Indicators by TrustLab, through our collaboration with EDMO, ERGA, Avaaz and the European Commission.
<p>Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]</p>	<p>Yes</p>
<p>If yes, which further implementation measures do you plan to put in place in the next 6 months?</p>	<p>We will continue to support the publication of Structural Indicators, and work towards further honing their methodology and scope.</p>
<p>Measure 41.1</p>	
<p>Measure 41.2</p>	
<p>Measure 41.3</p>	

X. Monitoring of Code

Commitment 42

Relevant Signatories commit to provide, in special situations like elections or crisis, upon request of the European Commission, proportionate and appropriate information and data, including ad-hoc specific reports and specific chapters within the regular monitoring, in accordance with the rapid response system established by the Taskforce.

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

Yes

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

We have been an active participant in the Crisis Response working group and have shared reports specific to the War of aggression by Russia on Ukraine and the Covid-19 pandemic along with this report.

Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]

Yes

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

We will continue to participate in the Crisis Response working group and share reports on topics aligned upon.

X. Monitoring of Code

Commitment 43

Signatories commit to produce reports and provide data following the harmonised reporting templates and refined methodology for reporting and data disclosure, as agreed in the Task-force.

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	<ul style="list-style-type: none">• Participated in the monitoring and reporting working group.• Provided timely feedback on the harmonized reporting template.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	We will continue to participate in the working group and contribute feedback to the report template.

X. Monitoring of Code

Commitment 44

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

In line with this commitment, did you deploy new implementation measures (e.g. changes to your terms of service, new tools, new policies, etc)? [Yes/No]	Yes
If yes, list these implementation measures here [short bullet points].	TikTok is committed to meeting its obligations under the DSA, including the independent audit obligations. We have taken steps to ensure readiness for our audit obligations including engaging with the European Commission's consultations on the audit requirements.
Do you plan to put further implementation measures in place in the next 6 months to substantially improve the maturity of the implementation of this commitment? [Yes/No]	Yes
If yes, which further implementation measures do you plan to put in place in the next 6 months?	TikTok is committed to meeting its obligations under the DSA, including the independent audit obligations. We will continue to take steps to ensure readiness for our audit obligations. We are also awaiting the relevant guidance from the Commission in order to finalise our compliance approach.

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

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

Covid-19 pandemic

Overview of the main threats observed, such as crisis related disinformation campaigns, spread of misinformation, coordinated manipulative behaviours, malicious use of advertising products, involvement of foreign state actors, etc.:

TikTok was pleased to learn in May 2023 that the WHO no longer considers Covid-19 a global health emergency as it reflects how much progress has been made in fighting against the virus. TikTok also welcomes the opportunity to provide this final Covid-19 related crisis report, setting out an overview of the threats we observed during the pandemic and the actions we took to mitigate related threats. Even with the WHO's determination in May, we have remained and are committed to remaining vigilant as to these threats and will continue to take actions to avoid the spread of misleading information in this context.

We continue to see a downward trend in our metrics in line with the de-escalation of Covid-19 as a global emergency. We also note that the number of Covid-19 vaccine tags are continuing to exceed Covid-19 notice tags, likely due to the fact that the vast majority of Covid-19 related content is now in relation to vaccines/vaccination.

We have still not seen any evidence of CIO on our platform as regards Covid-19 disinformation in the EU. We also have not observed coordinated attempts to influence or sway public opinion on Covid-19 pandemic while also misleading individuals, our community, or our systems about an account's identity, approximate location, relationships, popularity, or purpose.

TikTok's ad policy for Covid -19 related ads remains unchanged, with permitted ads generally coming from government authorities only. We are still seeing very few attempts to post ads related to Covid-19 or Covid-19 vaccines.

Executive summary of the company's main policies, strategies and actions taken to mitigate the identified threats and react to the crisis:

We continually work hard to ensure that TikTok is a source of reliable and safe information and we continue to recognise the heightened risk and impact of misleading information in the context of Covid-19.

Following the outbreak of the Covid-19 pandemic, we introduced several new policies to our Integrity & Authenticity Policies ([I&A policies](#)) including our Medical Misinformation policy, in order to respond to trends we witnessed and protect our users. We employ a layered approach to misinformation detection, leveraging multiple overlapping strategies to ensure comprehensive and responsive coverage and as part of this we have specialised misinformation moderation teams working to identify and remove such inaccurate, false or misleading content, as well as accounts that spread misinformation. This approach has enabled us to remove hundreds of thousands of videos containing misinformation related to the pandemic. At TikTok, we invest considerable resources in proactively identifying violative content, and so are proud that the vast majority of those videos were removed by us before they were reported by users or other third parties.. We also note that we recently made changes to our reporting feature to make the

“Misinformation” categories more intuitive and allow users to report misinformation with increased granularity.

Working closely with our fact-checking partners has been a crucial part of our approach to removing harmful medical misinformation from our platform. In particular, collaborating with certain of our fact-checking partners to receive advance warning of emerging misinformation narratives (including those related to vaccines and false cures) has facilitated proactive responses against high-harm trends and has ensured that our moderation teams have up-to-date guidance.

Recognising the importance of proactive measures, which are aimed at improving our users' digital literacy and increasing the prominence of authoritative information, we have continued our extensive in-app intervention measures (including video tags and search interventions) around Covid-19 and Covid-19 vaccine. We are proud to have partnered with a number of other experts in relation to the pandemic to share authoritative information with our users.

In relation to ads, we have our [Covid-19 ad policy](#), which prohibits ads which present Covid-19 in a distasteful manner e.g., manipulating consumers' fear or anxiety, or spreading harmful misinformation to push sales. We also promoted authoritative sources of information by providing free ad credits to health authorities, governments, and non-profits to increase vaccine adoption, debunk vaccine myths and promote trustworthy Covid-19 resources.

Best practices identified for future crisis situations:

- Working closely with our fact-checking partners and other experts to receive advance warning of emerging misinformation narratives. For TikTok, this facilitated proactive responses against high-harm trends and has ensured that our moderation teams have up-to-date guidance.
- Dedicating resources to increasing the number of in-app measures that show users additional context on certain content or redirect them to authoritative information.
- Rolling out media literacy campaigns in partnership with trusted organisations, focusing on addressing misinformation.

Future measures planned within the next six months:

- Continued expansion of our fact-checking network, consisting of committing to on-boarding new European-based fact-checking partners and increasing our operational coverage in the EEA. As part of these plans, we will be expanding our misinformation moderation teams.
- Continuing to work with our fact-checking partners to identify specific disinformation trends in countries and develop tailored, localised media literacy campaigns to tackle those trends.
- Continuing to redirect our users to authoritative, localised information from expert organisations (such as local public health sites or, where local health sites are not available, the WHO) when they interact with our dedicated Covid-19 notice tags and search intervention tools.

Changes in Policy Framework

	Policies	Rationale
--	----------	-----------

<p>Policies newly introduced for addressing the crisis</p>	<p>We have been able to rely on our existing, robust I&A policies as well as our dedicated advertising policies and as such have not needed to introduce new policies for the purposes of addressing the crisis.</p>	<p>In the context of the Covid-19 pandemic, we have been able to rely on our existing I&A policies which are our first line of defence in combating harmful misinformation and deceptive behaviours on our platform. These guidelines make clear to our users what content we remove or make ineligible for the For You feed when they pose a risk of harm to our users and their communities.</p> <p>Following the outbreak of the Covid-19 pandemic, we introduced several new policies to our I&A policies, in order to respond to trends we witnessed and protect our users. The policies we introduced, as well as examples as to the basis on which they have been enforced in relation to the crisis are as follows:</p> <ul style="list-style-type: none"> ● Medical misinformation Under this policy, we have been able to remove false claims about coronavirus, false cures and vaccine misinformation that could cause imminent harm to a user's health, or could cause harm to public health by discouraging people from seeking helpful medical treatment. ● Misinformation that induces panic about a crisis event or emergency. Under this policy, we have been able to remove content that is likely to stoke panic and consequently result in real world harm (e.g. content encouraging destruction of 5G towers by claiming they are spreading Covid-19). ● Dangerous conspiracy theories that are violent or hateful. In accordance with this community guideline and our hate speech policy, we have been able to remove content that suggests a certain race, ethnicity, gender or any member of a protected group is more susceptible to having and / or spreading Covid-19. <p>We have also supported our moderation teams with detailed policy guidance and direction when moderating on crisis related misinformation providing clarifications and updates as required. We have specialist teams within our Trust and Safety department dedicated to the policy issue of I&A including within the areas of product and policy. Our experienced subject matter experts on I&A continually keep these policies under review and collaborate with external partners and experts when understanding whether updates are required.</p> <p>In an ads context, we have been able to rely on our Covid-19 ad policy which prohibits ads which present Covid-19 in a distasteful manner, which includes spreading harmful misinformation to push sales.</p>
<p>Policies adapted for addressing the crisis</p>	<p>Since the beginning of the reporting period, we have not adapted our Terms of Service or CGs for addressing the crisis, as</p>	<p>See rationale above.</p>

	<p>we have been able to rely on the I&A policies as well as our dedicated ad policies as an effective basis for tackling content related to the pandemic.</p> <p>However, we have recently refreshed our CGs to increase transparency to our users.</p>	
Policies regarding the crisis repealed/removed	We have not removed or repealed any policies related to the crisis.	

Reporting on the service's response during a period of crisis
War of aggression by Russia on Ukraine
<p>Overview of the main threats observed, such as crisis related disinformation campaigns, spread of misinformation, coordinated manipulative behaviours, malicious use of advertising products, involvement of foreign state actors, etc.:</p> <p>The war of aggression by Russia on Ukraine is devastating, and, as a platform, has challenged us to confront a complex and rapidly changing environment. At TikTok, the safety of our people and community is of paramount importance and we work continuously to safeguard our platform.</p> <p>We have set out below some of the main threats we have observed on our platform in relation to the spread of harmful misinformation and covert influence operations (CIO) related to the war and note that we are committed to taking action to prevent such content from being shared in this context.</p> <p><u>(I) Spread of harmful misinformation</u></p> <p>We continue to observe and take action where appropriate under our policies. In terms of trends observed, we have seen false or unconfirmed claims about specific attacks and events, the development or use of weapons, the involvement of specific countries in the conflict and statements about specific military activities, such as the direction of troop movement. We also have seen instances of footage repurposed in a misleading way, including from video games or unrelated footage from past events presented as current.</p>

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

(II) CIOs

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

We have confirmed that during the period from September 2022 to March 2023, we took action to remove a total of 6 networks (consisting of 4932 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. We publish all of the CIO networks we identify and remove within our transparency reports, [here](#).

We know that CIO will continue to evolve in response to our detection and networks may attempt to 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.

Executive summary of the company's main strategies and actions taken to mitigate the identified threats and react to the crisis:

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

(I) Investment in our fact-checking program

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

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

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

(II) Disruption of CIOs

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

Between September 2022 and March 2023, we took action to remove a total of 6 networks (consisting of 4932 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. We publish all of the CIO networks we identify and remove within our transparency reports, [here](#).

(III) Restricting access to content for state affiliated media

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

Since January 2023, we have scaled up our detection and labelling of state-controlled media accounts following the roll-out of our state-controlled media label policy globally. We are committed to further expansion.

(IV) Mitigating the risk of monetisation of harmful misinformation

Whilst we have long prohibited political advertising on our platform, we have taken measures to further mitigate the risk of monetisation off the back of the war by disallowing Ukrainian and Russian advertisers from targeting EU markets and removing Livestream videos originating in Russia and Ukraine from the For You feed of users located in the EU.

(V) Launching localised media literacy campaigns

Lastly, recognising the importance of proactive measures which are aimed at improving our users' digital literacy and increasing the prominence of authoritative information, we developed and launched eight localised media literacy campaigns addressing disinformation related to the war on Ukraine in PL, SK, RO, UA, HU, EE, LT, and LV, in close collaboration with our fact-checking partners. Users searching for keywords relating to the war 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.

Best practices identified for future crisis situations:

- Working closely with our 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.
- Dedicating resources to increasing the number of in-app measures that show users additional context on certain content or redirect them to authoritative information.
- Rolling out media literacy campaigns in partnership with trusted organisations, focusing on addressing disinformation.

Future measures planned within the next six months:

- Continued expansion of our fact-checking network, consisting of committing to on-boarding new European-based fact-checking partners and increasing our operational coverage in the EEA (and expanding our misinformation moderation teams accordingly).
- Continuing to work with our fact-checking partners to identify specific disinformation trends in countries and develop tailored, localised media literacy campaigns to tackle those trends and developing our fact-checking repository to ensure our teams and systems leverage the full scope of insights our fact-checking partners submitted to TikTok. We will also continue to participate in the sub-group on the creation of an external repository.
- Continuing the detection and labelling of state-controlled media in Europe and expanding the policy further globally.
- Continuing to explore ways to expand the use cases of our unverified content label.
- Following consultations with researchers, exploring and considering how we engage with users who have interacted with harmful misinformation on our platform and direct them to authoritative information.
- Continuing to strengthen how we enforce our synthetic media policy and exploring new products and initiatives to help enhance our detection and enforcement capabilities in relation to our synthetic media policy, including user education initiatives.

[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 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].

Changes in Policy Framework

	Policies	Rationale
--	-----------------	------------------

<p>Policies newly introduced for addressing the crisis</p>	<p>We continue to rely on our existing, robust I&A policies and as such have not needed to introduce new policies for the purposes of addressing the crisis.</p> <p>However, since the previous reporting period, we have refreshed our CGs to increase transparency for users and provide more specific examples. As part of this we launched our updated synthetic media policy to address the use of content created or modified by AI technology on our platform.</p>	<p>In the context of the war, we have been able to rely on our I&A policies, which are our first line of defence in combating harmful misinformation and deceptive behaviours on our platform.</p> <p>These guidelines make clear to our users what content we remove or make ineligible for the For You feed when they pose a risk of harm to our users or the wider public. We have also supported our moderation teams with detailed policy guidance and direction when moderating on 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 I&A, including within the areas of product and policy. Our experienced subject matter experts on I&A continually keep these policies under review and collaborate with external partners and experts when understanding whether updates are required.</p> <p>When situations such as the war in Ukraine arise, these teams work to ensure that appropriate guidance is developed so that the I&A policies are applied in an effective manner in respect of content relating to the relevant crisis (in this case, the war). This includes issuing detailed policy guidance and direction, including providing case banks on harmful misinformation claims to support moderation teams.</p>
<p>Policies adapted for addressing the crisis</p>	<p>Since the beginning of the reporting period, we have been able to rely on the I&A policies, which are an effective basis for tackling content related to the war. As such, we have not adapted our Terms of Service or CGs for addressing the crisis. In a crisis, we keep under review our policies and to ensure moderation teams have supplementary guidance.</p>	<p>See rationale above.</p>
<p style="text-align: center;">Actions to mitigate the crisis impact on the service</p>		

Type of mitigation	Intervention or action (short summary) [suggested character limit: 500 characters]	Intervention or action (explanation and implementation) [suggested character limit: 2000 characters]	Impact metrics
<p>Actions taken against dis- and misinformation content (for example deamplification, labelling, removal etc.)</p>	<p><u>Removing harmful misinformation from our platform</u></p> <p>Since the outbreak of the war, we have removed tens of thousands of videos containing harmful misinformation related to the war from our platform.</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>We take action to remove accounts or content which 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 which makes false and harmful claims about specific events, or incites panic. In certain circumstances, we may also reduce the prominence of such content.</p> <p>We employ a layered approach to misinformation detection, leveraging multiple overlapping strategies to ensure comprehensive and responsive coverage. We place considerable emphasis on proactive content moderation strategies in order to remove harmful misinformation which is in violation of our policies before it is reported to us by users or third parties.</p> <p>In the context of the crisis, we are proud to have proactively removed tens of thousands of videos containing harmful misinformation</p>	<p>Number of videos removed because of violation of misinformation policy with a proxy related to the War of Aggression by Russia on Ukraine - 8,358</p> <p>Number of proactive removals of videos removed because of violation of misinformation policy with a proxy related to the War of Aggression by Russia on Ukraine - 7,034</p>

		<p>related to the war. We have been able to do this through a combination of automated review, - human level content moderation, carrying out targeted sweeps of certain types of content (e.g. hashtags/sensitive keyword lists) as well as working closely with our fact-checking partners and responding to emerging trends they identify.</p> <p>We have invested heavily in Russian and Ukrainian native language speakers for content moderation, as we recognise the importance of local cultural and linguistic context in the misinformation moderation process.</p>	
	<p><u>Applying our state affiliated media label</u></p> <p>We have restricted access to certain state-affiliated media entities and expedited the roll-out of our state-affiliated media policy and label in order to bring viewers context to evaluate content shared by such Russian, Ukrainian and Belarusian entities.</p>	<p>In the EU, Iceland and Liechtenstein, we have taken steps to restrict access to content from the following entities: Russia Today; Sputnik; Rossiya RTR/RTR Planeta; Rossiya 24/Russia 24; and TV Centre International.</p> <p>We have also expedited the roll out of our state-affiliated media policy in order to bring viewers context to evaluate the content they consume on our platform in relation to the war and labels have since been applied to content posted by the accounts of such entities in Russia, Ukraine and Belarus.</p> <p>Since January 2023, we have</p>	<p>Number of videos tagged with the state affiliated media label for Russia, Belarus and Ukraine - 79,553</p> <p>Number of impressions of the state affiliated media label for Russia, Belarus and Ukraine - 19,348,840</p>

		<p>scaled up our detection and labelling of state-controlled media accounts following the roll-out of our state-controlled media label policy globally. We are committed to further expansion.</p> <p>Where the label is applied to content, 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>Promotion of authoritative information, including via recommender systems and products and features such as banners and panels</p>	<p><u>Not proactively promoting news-type content to our users</u></p> <p>We do not actively promote news-type content, such as news related to the war, on our platform. Our recommender system is personalised based on user engagement, so if a user engages with news-type content, it may be the case that more of such content will appear over time, but it will not be actively promoted by us.</p>	<p>TikTok is primarily an entertainment platform. It may be the case that a user’s For You feed shows more news-type content (such as news content relating to the war) over time if that is content that a user is actively looking for and engaging with, but we do not actively promote news content to users on TikTok.</p> <p>Further, TikTok’s recommender system delivers a personalised feed of content based on a user’s engagement behaviour with video content types. Every user’s feed will look different, according to their own preferences, which are demonstrated through ‘likes’, watch duration and other related metrics. For more information on how our</p>	<p>N/A</p>

	<p><u>Applying our unverified content label to make content ineligible for recommendation</u></p> <p>Where our specialised 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 crisis), 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 misleading information.</p>	<p>recommendation system works, see here.</p> <p>Verifying certain information during dynamic and fast moving events such as a war can be challenging and our moderators and fact-checkers cannot always conclusively determine whether content is indeed harmful misinformation, in violation of our CGs.</p> <p>Therefore, in order to minimise risk, where our fact-checkers or our specialised 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>N/A</p>
--	---	---	------------

	<p><u>Removing Russian and Ukrainian Livestream content from the For You feed of EU users.</u></p> <p>We have taken action to remove Livestream videos originating in Russia and Ukraine from the For You feed of users located in the EU and suspend new content creation from our video service in Russia in light of their new "fake news" law.</p>	<p>We have removed Livestream videos originating in Russia and Ukraine from the For You feed of users located in the EU. This has been done in order to minimise the risk of harmful content appearing in a user's feed and given the uptick of Livestreams from that region since the outbreak of the war.</p> <p>We also swiftly took action to suspend new content creation from our video service in Russia in order to review the safety implications of the "fake news" law which was passed by the Russian parliament in March 2022.</p>	<p>N/A</p>
	<p><u>Creating localised media literacy campaigns</u></p> <p>We launched localised media literacy campaigns relating to the crisis in order to raise awareness amongst our users. We promoted the campaign through a combination of our in-app intervention tools in order to ensure that authoritative information is promoted to our users</p>	<p>We recognise the importance of proactive measures which are aimed at improving our users' digital literacy and increasing the prominence of authoritative information.</p> <p>Working with our fact-checking partners, this year we have developed and rolled-out eight localised media literacy campaigns on the war in Poland, Slovakia, Romania, Ukraine, Hungary, Estonia, Latvia and Lithuania.</p> <p>Users searching for keywords relating to the war are directed to tips, prepared in partnership with our fact checking partners, to help users identify misinformation and</p>	<p>Total number of impressions of the Fakenews.pl Campaign Page in EEA - 108,109</p>

		prevent the spread of it on the platform.	
<p>Cooperation with independent fact-checkers in the crisis context, including coverage in the EU</p>	<p><u>Ensuring fact-checking coverage</u></p> <p>Our fact checking efforts cover Russian, Ukrainian, Belarusian and all major European languages (including 17 official European languages as well as a number of other languages which affect European users).</p>	<p>We see harmful misinformation as different from other content issues. Context and fact-checking are critical to consistently and accurately enforcing our harmful misinformation policies, which is why we have ensured that, in the context of the crisis, our fact-checking programme covers Russian, Ukrainian and Belarusian.</p> <p>More generally, we work with 9-fact-checking partners in Europe, covering the spoken language of 22 EEA countries (as well as a number of other languages which affect European users). We recently onboarded a new fact-checking partner, Reuters, who are dedicated to fact-checking content in Russian and Ukrainian. To further support our fact-checking efforts in Ukraine specifically, we have also been leveraging additional Ukrainian-speaking reporters who are connected with some of our existing fact checking partners.</p> <p>We are committed to expanding our fact-checking program by on-boarding new European-based fact-checking partners and increasing our operational coverage in the EEA (and expanding our misinformation moderation teams accordingly).</p>	<p>Number of fact checked videos with a proxy related to the War of Aggression by Russia on Ukraine - 832</p> <p>Number of videos removed as a result of a fact checking assessment with words related to RU/UA - 211</p>

	<p><u>Collaborating with our fact-checking partners in relation to emerging trends</u></p> <p>We have engaged with our fact-checking partners to understand and receive advance notice of emerging misinformation trends in order to ensure that our moderation teams are well-equipped to take action.</p>	<p>Since the beginning of the crisis, representatives from TikTok's misinformation policy and detection teams have met regularly with our external fact-checking partners, to receive advance warning of emerging misinformation narratives, facilitating proactive responses against high-harm trends.</p>	<p>Number of videos removed because of policy guidelines, known misinformation trends and knowledge based repository with words related to RU/UA - 8,358</p>
<p>Measures taken to demonetise disinformation related to the crisis</p>	<p><u>Prohibiting political advertising and monetisation related to the war from our platform</u></p>	<p>We do not allow political advertising from anyone, including from state media, on our platform. More specifically, and as outlined in our ad policy, we do not permit ads for the promotion, reference, or opposition of: a candidate for public</p>	<p>N/A</p>

		<p>office, a current or former political leader, political party, or political organisation, content that advocates a stance (for or against) on a local, state, or federal issue of public importance in order to influence a political decision or outcome.</p> <p>As mentioned previously, our monetisation integrity content teams observed a sharp rise in attempts to post ads related to political/war content during the initial period of the conflict commencement. Our risk control methods ensured there was no corresponding increase in violating activity going live on the platform. Since the initial period of the conflict, these numbers have significantly dropped. We have since seen no additional spike.</p> <p>Since the beginning of the war, we have taken a strict position not to enable associated monetisation. This includes direct monetisation (e.g. the sale of merchandise associated with the war) as well as any reference to the war. Since March 2022, we have not allowed Ukrainian and Russian based advertisers to target EU markets.</p>	
<p>Measures taken to prevent malicious advertising</p>	<p><u>Content moderation</u></p> <p>We use a combination of automated and human moderation</p>	<p>We enforce our strict ad policies with a combination of automated and human moderation, and have expert teams focused on</p>	<p>N/A</p>

	<p>in order to identify content that breaches our ad policies.</p>	<p>investigating and responding to any attempts to circumvent our policies.</p> <p>Our Monetisation Integrity department has moderation teams in multiple locations that speak Russian and Ukrainian.</p> <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>Measures taken in the context of the crisis to counter manipulative behaviours/TTCs</p>	<p><u>Identifying and removing CIO networks</u></p> <p>Our dedicated investigation teams and automated systems have been on high alert to identify threats related to CIO networks and have removed networks targeting discourse about the war in Ukraine, in accordance with our I&A policies which prohibit deceptive behaviours.</p>	<p>We fight against CIO as our I&A policies prohibit attempts to sway public opinion while also misleading our systems or users about the identity, origin, approximate location, popularity or overall purpose. We have specifically-trained teams which are on high alert to investigate and detect CIO networks on our platform.</p> <p>Between September 2022 and March 2023, we took action to remove a total of 6 networks (consisting of 4932 accounts in total) that were found to be involved in coordinated attempts to influence public opinion about the Russia-Ukraine war while also misleading individuals, our community, or our systems.</p> <p>We published this information within our most recently published transparency report, here.</p>	<p><i>NB:</i> <i>We are only able to provide the Q4 2022 and Q1 2023. We are building and testing data infrastructure that can provide information requested at a high level of fidelity. Additionally, CIO network investigations are highly resource heavy requiring in depth analysis to ensure high confidence in proposed actions. We publish all of the CIO networks we identify and remove within our transparency reports, here.</i></p> <p>The following networks targeting discourse around the Russia-Ukraine War were removed between September 2022 and March 2023:</p> <p>In Q4 2022:</p> <ul style="list-style-type: none"> ● We assessed that a network operated from Russia and targeted European countries, primarily Germany. The individuals behind these accounts created inauthentic accounts and shared inauthentic localised content in German about the ongoing war in Ukraine, as well as its consequences on EU countries' economies. <ul style="list-style-type: none"> ○ Accounts in network: 3,181 ○ Followers of network: 418,196

		<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>In Q1 2023:</p> <ul style="list-style-type: none"> ● We assessed that a network operated from Russia and targeted primarily Russian audiences. The network was partially created prior to our suspending live streaming and new content in Russia and extensively used location obfuscation as a tactic. The individuals behind this network used inauthentic identities, including inauthentic news outlets, in order to artificially amplify a pro-Russia viewpoint targeting discourse about the war in Ukraine. <ul style="list-style-type: none"> ○ Accounts in network: 15 ○ Followers of network: 38,326 ● We assessed that a network operated from Russia and targeted Russian audiences. The network extensively used location obfuscation as a tactic to mislead TikTok’s systems. The individuals behind this network used inauthentic accounts to hyper-post content in order to artificially promote Yevgeny Viktorovich Prigozhin’s war film “The Best in Hell”, <ul style="list-style-type: none"> ○ Accounts in network: 254 ○ Followers of network: 34,110 ● We assessed that a network operated from Russia and targeted Russian audiences. The individuals behind this network created inauthentic accounts and hyper-posted content with the aim of artificially amplifying specific pro-Russia viewpoints in the context
--	--	--	--

			<p>of the war in Ukraine, abusing the re-share function and using the web application in order to circumvent the regional TikTok ban in Russia.</p> <ul style="list-style-type: none"> ○ Accounts in network: 1,351 ○ Followers of network: 226,838 <ul style="list-style-type: none"> ● We assessed that a network operated from Russia and targeted various European countries such as Germany, Italy, and the UK. The individuals behind this network used impersonation in order to artificially amplify specific viewpoints related to Ukraine's president Zelensky, the economic sanctions currently imposed on Russia, and Ukrainian refugees. <ul style="list-style-type: none"> ○ Accounts in network: 12 ○ Followers of network: 1,480 ● We assessed that a network operated from Ukraine and targeted Ukrainian audiences. The individuals behind this network created inauthentic accounts and hyper-posted content with the aim of artificially amplifying specific viewpoints related to the Ukrainian government and of promoting a positive image of President Zelensky. <ul style="list-style-type: none"> ○ Accounts in network: 119 ○ Followers of network: 90,303
	<p><u>Tackling synthetic media</u></p> <p>We recently launched our synthetic media policy to address</p>	<p>Our synthetic media policy requires deceptive or synthetic media that shows realistic scenes must be clearly disclosed.</p>	<p>N/A</p>

	<p>the use of manipulated and AI-generated media on our platform.</p>	<p>For the purposes of our policy, synthetic media refers to content created or modified by AI technology. It includes highly realistic digitally-created (fake) content of real people, such as a video of a real person speaking but their words have been modified or changed.</p> <p>Prohibited practices are set out in our I&A policies here.</p>	
<p>Measures taken to support research into crisis related misinformation and disinformation</p>	<p>We have not been involved in any research initiatives in the context of the war to date, however, we are committed to engaging with researchers going forwards.</p>	<p>We have not been involved in any research initiatives in the context of the war to date.</p> <p>We recently launched our Research API which is designed to provide researchers with access to certain public data on content, accounts and comments from our platform.</p>	<p>N/A</p>
<p>Relevant changes to working practices to respond to the demands of the crisis situation and/or additional human resources procured for the</p>	<p>We have continued to invest in localised moderation capabilities.</p>	<p>We have continued to invest within the region, including Russian and Ukrainian native language speakers for content moderation, and this investment has been significantly increased since the war began.</p>	<p>This is a dynamic situation, and we also leverage the capabilities of fact-checking partners, so numbers can fluctuate.</p>

mitigation of the crisis			
--------------------------	--	--	--