

Code of Practice on
Disinformation – Report
of CEE Digital
Democracy Watch
(Fundacja
Obserwatorium
Demokracji Cyfrowej for
the period 1 January to
30 June 2025

Reporting on the service's
response during an election

Reporting on the service's response during an election

Threats observed or anticipated at time of reporting:

In the run-up to the Polish presidential election, one of the central concerns was the absence of a Digital Services Coordinator (DSC) in Poland. This meant that enforcement of DSA obligations for Very Large Online Platforms (VLOPs) relied solely on the European Commission, without a national authority empowered to monitor platform compliance or provide rapid response during campaigns.

Experiences from previous Polish electoral cycles highlighted the systemic risks linked to online campaigning. Reports from previous campaigns showed use of opaque political advertising, including influencer partnerships and microtargeted content, with limited transparency on spending sources.

Given the proximity to Russian aggression Ukraine, Poland became a target of sustained information operations. EU and NATO threat assessments repeatedly underlined Poland as one of the main theaters of Russian disinformation in Europe.

Concerns about low content moderation capacity in local languages were also a risk factor. While major platforms declare the presence of moderators for Polish-language content, transparency reports and expert analyses reveal that actual human moderation resources remain limited compared to the volume of content produced.

Mitigations in place – or planned - at time of reporting:

As a new signatory to the Code, and with the goal of preparing for the Polish elections, our organisation participated as an observer in monitoring the Romanian elections a few weeks prior to the launch of the Polish RRS.

Before the campaign, our team also raised questions on digital threats to elections during the selection process for the new Head of the National Election Bureau in Poland.

Within the framework of the RRS, our organisation flagged a over a dozen pieces of content, with the majority of reports concerning TikTok accounts spreading election misinformation and hate speech.

We also submitted situational reports and general observations, highlighting potential infringements in the use of platform tools. These included the absence of archiving and analysis of TikTok's Live function, the lack of transparency in X's political advertising system, and the insufficient clarity of ad labelling by Meta.

Beyond participation in meetings and reporting, our organisation played an active role in informing the public and stakeholders. We published a weekly report summarising the ten largest political advertising campaigns across Meta and Google platforms, which was further disseminated through our partners' communication channels.

We also issued fortnightly data reports on the online activity of Polish political leaders across five social media platforms (X, Google, Facebook, Instagram, TikTok), which were regularly shared with relevant stakeholders.

In the run-up to the elections, CEE DDW advocated for establishing a pre-election stress test by the Polish government. We also participated in civic organisation briefings hosted by NASK under the Election Umbrella initiative and in election integrity briefings prepared by platforms such as Meta and TikTok.

Additionally, we were an active member of cross-border watchdog networks, engaging through forums such as Alliance4Europe's Counter Disinformation Network.

During the election, we promoted awareness of digital threats and the DSA's role through appearances in Tier 1 Polish media. In the final phase of the voting process, our representatives also met with election observation missions from the OSCE and the Parliamentary Assembly of the Council of Europe.

Positive experiences gained through the RRS process were later shared with the European campaigning community in the form of a webinars hosted by EPDE or Political Tech Summit.

A key takeaway from the RRS work was the submission of detailed feedback on two technical documents implementing the Regulation on the Targeting and Transparency of Political Advertising.

Our recommendations focused on ensuring the labels remain unchanged between account verification and ad broadcast, stressed that public labels must consistently present the original verified data and recommended automatic shutdown mechanisms for restricted ads during election periods.

Our work was also reflected in policy brief for the Institute for Public Affairs available [here](#).

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

Scrutiny of Ads Placements

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

Specific Action applied (with reference to the Code's relevant Commitment and Measure)

Specific Action applied (with reference to the Code's relevant Commitment and Measure)

Political Advertising

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

Specific Action applied (with reference to the Code's relevant Commitment and Measure)

Publication of weekly report summarising the ten largest political advertising campaigns across Meta and Google platforms, which was further disseminated through our partners' communication channels.

Integrity of Services

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

Specific Action applied (with reference to the Code's relevant Commitment and Measure)

Publication of fortnightly data reports on the online activity of Polish political leaders across five social media platforms (X, Google, Facebook, Instagram, TikTok), which were regularly shared with relevant stakeholders.

Empowering Users	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	NA
	NA
Empowering the Research Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	NA
	NA
Empowering the Fact-Checking Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	NA
	NA