European Digital Media Observatory

European Digital Media Observatory

# Lessons Learned from Six National Elections

Inputs for the Review of the DSA Election Guidelines

October 2026

## Lessons Learned from Six National Elections


**1. Introduction** 3
**2. Romania – Presidential Elections, May 2025 (BROD)** 4
2.1 Context and monitoring activities 4
2.2 Main findings and platform shortcomings 4
2.3 Recommendations for platforms 5
2.4 Recommendations for the DSA Election Guidelines 5
**3. Moldova – Parliamentary Elections, September 2025 (FACT)** 7
3.1 Context and monitoring activities 7
3.2 Main findings and platform shortcomings 7
3.3 Recommendations for platforms and EU institutions 7
3.4 Recommendation for the RRS 8
**4. Hungary – Parliamentary Elections, April 2026 (HDMO)** 9
4.1 Context and monitoring activities 9
4.2 Main findings and platform shortcomings 9
4.3 Recommendations for platforms 11
4.4 Recommendations for the DSA Election Guidelines 11
**5. Bulgaria – Parliamentary Elections, April 2026 (BROD)** 13
5.1 Context and monitoring activities 13
5.2 Main findings and platform shortcomings 13
5.3 Recent developments: autumn 2026 presidential campaign 14
5.4 Results of the MVI pilot and third evaluation report 14
5.5 Recommendations for platforms 15
5.6 Recommendations for the DSA Election Guidelines 15
**6. Cyprus – Parliamentary Elections, May 2026 (MEDDMO)** 16
6.1 Context and monitoring activities 16
6.2 Main findings and platform shortcomings 16
6.3 Recommendations for platforms 17
6.4 Recommendations for the RRS and election coordination 17
**7. Malta – General Election, May 2026 (MEDDMO)** 18
7.1 Context and monitoring activities 18
7.2 Main findings and platform shortcomings 18
7.3 Recommendations for platforms 19
7.4 Recommendations for the RRS and election coordination 19
**8. Conclusions** 20
**9. Original contributions** 22



The European Digital Media Observatory has received funding from the European Union under project number 300141274.

# 1. Introduction

EDMO and its network of national and regional Hubs have extensive experience monitoring and countering disinformation before, during and after elections across EU Member States and beyond.

This report draws on four EDMO Hubs' experience across six recent high-stakes elections and their contributions to the EDMO Taskforce for Elections and Crisis-Related Disinformation. The Taskforce became operational at the end of April 2026, building on existing cooperation between EDMO.eu, which entered its third phase in March 2026, and the relevant Hubs. This included guidance on the Rapid Response System (RRS) under the Code of Practice on Disinformation, now the Code of Conduct, particularly during the April 2026 elections in Hungary (covered by HDMO) and Bulgaria (BROD).

The report also covers the May 2026 general elections in Malta and Cyprus, monitored by MedDMO, and the 2025 elections in Moldova and Romania. Although the latter preceded the Taskforce's establishment, FACT and BROD shared their findings with the wider EDMO network and received support from EDMO.eu, particularly on the RRS. Other elections covered by the EDMO Taskforce, such as those in Denmark, Sweden and Latvia, were not significantly affected by disinformation campaigns on social media and are therefore not included in the report.

Focusing on social media and online platforms, the report identifies lessons learned through the RRS and areas where EU-level action could improve platforms' efforts to counter disinformation and inform the revision of the DSA Election Guidelines.

One important caveat: platforms often respond to disinformation-related issues reported by organizations within the EDMO network by removing content. As EDMO, we neither endorse nor support this practice. We believe that a better approach is to label content and inform the public about what is false or misleading and why. When platforms remove content without explaining the reasons for doing so, as often happens, this makes the situation even worse and can undermine the effectiveness of the remedy, fuelling the spread of further conspiracy theories and disinformation about the removals themselves.

Moreover, targeting content is not only problematic but also less effective than targeting accounts. Bots are not real people and therefore have no human rights of their own to protect. Accounts operated by real people who systematically violate the law and platform rules, on the other hand, should be sanctioned, as they would be in the offline world, in order to protect other users and deter criminal and predatory behaviour.

# 2. Romania – Presidential Elections, May 2025 (BROD)

## 2.1 Context and monitoring activities

Romania's presidential re-run, held on 4 and 18 May 2025, showed that the manipulation infrastructure behind the annulled 2024 election remained largely intact. Platforms addressed individual items without dismantling the networks responsible for producing and amplifying them.

Between 25 March and 20 May 2025, BROD and Funky Citizens monitored TikTok, Meta and X, flagged 26,613 posts, analysed 69,529 comments on 92 posts by the two run-off candidates, and submitted 4,773 RRS notifications. Findings were published in 11 weekly bulletins and a final status report.

## 2.2 Main findings and platform shortcomings

Platforms took action in respect of 68.4% of flagged posts, by removing the problematic content. However, only 6 of 251 TikTok accounts reported for suspected inauthentic behaviour had been deactivated by 29 May 2025 (2.4%).

1. **Content removal without network disruption.** Platforms removed individual items while the accounts producing them remained active. The same infrastructure re-emerged at politically sensitive moments between 2024 and 2025.
2. **Uneven enforcement.** TikTok removed over 1,000 items of illegal voting-booth footage, 323 election-rigging claims, 228 antisemitic posts and 177 smear posts, yet similar content remained online. Meta's remedial actions were minimal and X was virtually non-responsive.
3. **Artificial engagement and recommender systems.** Suspicious accounts displayed linguistic anomalies, implausible geographic origins and synchronised growth in candidate engagement, without evidence that algorithms adequately discounted this activity. Researchers identified 286 suspicious TikTok accounts amplifying George Simion (leader of the far-right party “Alliance for the Union of Romanians” - AUR),and 135 amplifying Nicușor Dan (President of Romania).
4. **Undisclosed political promotion.** Influencer networks, including those operating through FameUp, and pages with undisclosed ownership promoted political content without effective advertising labels or campaign finance oversight. Investigative journalists documented anonymous Facebook pages spending over €60,000 on unlabelled political advertisements during the first campaign week.

5. **Cross-platform amplification.** Narratives moved from Telegram groups to TikTok, Facebook and fringe websites. Monitoring covered over 9,000 posts from 35 campaign-affiliated Telegram groups, but platforms assessed only their own segments.
6. **AI-generated content and impersonation.** Deepfakes and fabricated diplomas targeted Nicușor Dan. Cloned websites impersonating Romanian institutions and media used AI-generated content and native advertising services previously associated with Russian influence efforts.
7. **Insufficient Romanian-language moderation.** Limited moderation capacity left narratives targeting Moldovan voters and the Romanian-speaking diaspora inadequately addressed.
8. **Limited RRS impact on coordinated inauthentic behaviour (CIB).** Platforms responded to all 4,773 notifications, an improvement on 2024, but documented networks and artificial boosts involving millions of likes and views prompted no concrete action or explanation.

## 2.3 Recommendations for platforms

1. **Prioritise account- and network-level enforcement:** investigate reported CIB, act against persistent networks and explain to flaggers which accounts were reviewed and why.
2. **Discount inauthentic engagement:** down-rank content boosted by accounts showing linguistic anomalies, implausible geography, synchronised activity or reactivation after dormancy.
3. **Increase small-language moderation capacity:** deploy native speakers with regional political knowledge, including across Romania and Moldova.
4. **Address undisclosed political promotion:** detect paid influencer content and political activity by pages with undisclosed ownership.
5. **Improve cross-platform information sharing:** exchange indicators of coordinated operations seeded on one service and amplified on others.
6. **Detect and label AI-generated electoral content:** address candidate deepfakes and impersonation of institutions and media.
7. **Provide timely researcher access:** make usable data available to vetted researchers and civil society before campaigns begin.

## 2.4 Recommendations for the DSA Election Guidelines

1. **Address long-term audience priming.** Narratives about a “parallel state”, EU interference and imminent war circulated for years. Risk assessments should begin well before official campaigns and cover sustained, low-intensity amplification. **Activate the RRS earlier,** before manipulation reaches critical mass.
2. **Require election-specific enforcement reports** covering content and account actions, response times, civil society and authority reports, and feedback on CIB cases.

3. **Clarify the interaction between the DSA and national electoral law.** Romania's Emergency Ordinance 1/2025 and 178 Central Electoral Bureau removal decisions, some targeting private individuals classified as “political actors”, raised freedom of expression concerns. Guidance should reduce the risk of over-enforcement.
4. **Strengthen cross-border coordination.** As operators treat Romania, Moldova and Bulgaria as one operational space, the Guidelines should facilitate information sharing among Digital Services Coordinators and EDMO Hubs.
5. **Safeguard independent monitors.** Funky Citizens and Factual faced campaigns portraying RRS participation as “censorship”, amplified by a February 2026 U.S. House Judiciary Committee report. The Guidelines should clarify that flaggers provide analysis while platforms decide on enforcement, and recognise the delegitimisation of monitors as a systemic risk.

# 3. Moldova – Parliamentary Elections, September 2025 (FACT)

## 3.1 Context and monitoring activities

FACT's monitoring in Moldova, Romania and Hungary highlighted delayed action against CIB, inconsistent treatment of monitoring content and limited access to platform data.

## 3.2 Main findings and platform shortcomings

1. **Delayed enforcement.** Many TikTok accounts and posts reported during elections in Moldova, Romania and Hungary were removed only at the end of the campaign. In Hungary, TikTok did not respond to a large CIB dataset flagged with support from Alliance4Europe.
2. **Inconsistent treatment of monitoring content.** In Romania, CIB reports did not lead to its removal, while Facebook removed the monitoring organisation's journalistic and informational content about the case. Restoration and a response took several days.
3. **Persistent CIB networks.** FACT documented over 100 TikTok accounts in Moldova that had engaged in CIB for at least nine months before the election. A benefiting politician's account continued displaying the same pattern without action.
4. **Limited investigative capacity.** Platforms described CIB investigations as difficult. Some relied on manual review of individual items, while Facebook's removal of FACT's own content appeared automated.
5. **Insufficient platform and financial data.** A data leak showed that some TikTok influencer and politician accounts had over 50% of followers associated with IP addresses outside Moldova. FACT called for greater EDMO Hub access to relevant user and financial data under the DSA and RRS, citing TikTok's processing of €400 million in Romania as an example of insufficiently transparent financial activity.

## 3.3 Recommendations for platforms and EU institutions

1. **Investigate CIB at network level,** including persistent networks identified before elections.
2. **Apply consistent standards** to reported manipulation and journalistic content documenting it.
3. **Explain investigative procedures and decisions,** providing meaningful feedback to flaggers.

4. **Expand safeguarded EDMO Hub access** to platform user data needed to investigate coordinated and cross-border operations.
5. **Improve access to financial data r**elevant to platform activity, advertising and commercial operations.

## 3.4 Recommendation for the RRS

The RRS should begin at least six months before election day to enable early identification and investigation of coordinated networks.

# 4. Hungary – Parliamentary Elections, April 2026 (HDMO)

## 4.1 Context and monitoring activities

During the Hungarian parliamentary election campaign, HDMO monitored political advertising, AI-generated content and coordinated inauthentic behaviour (CIB). Its contributing organisations, Political Capital and Lakmusz, reported suspected platform-policy violations and potential DSA breaches to Meta, Google and TikTok.

Ahead of the 12 April 2026 election, the signatories to the Code of Conduct on Disinformation activated the Rapid Response System (RRS). HDMO participated as an EDMO Hub, with support from EDMO.eu and the wider network, flagging political advertisements, suspected coordinated networks, persistent fake profiles and inadequately labelled AI-generated content.

The monitoring took place after major platforms introduced EU-wide restrictions on political advertising in autumn 2025. Despite the ban on political advertising, pro-government actors and affiliated organisations continued promoting political content by exploiting classification and enforcement weaknesses. AI-generated videos and deepfakes targeting the main opposition leader also reached millions through paid promotion.

## 4.2 Main findings and platform shortcomings

1. **Political advertising restrictions were circumvented.** Meta and Google continued to allow political content to be promoted as non-political, including advertisements using indirect references or omitting explicit political identifiers. Google classified political ads under unrelated categories such as Arts and Entertainment, Finance, and Internet and Telecom; identical or similar advertisements could receive different labels or be reclassified. Government advertisements against political opponents appeared across Google, Meta and billboards, while the Meta version omitted the face of European Commission President Ursula von der Leyen. These inconsistencies undermined the effectiveness and verifiability of the restrictions.
2. **AI-generated political content achieved substantial paid reach.** Government-controlled media, politicians and government-organised non-governmental organisations (GONGOs) used AI-generated images and videos extensively. The National Resistance Movement (NEM), a government-affiliated proxy organisation, published animated political advertisements and deepfakes discrediting the main opposition leader. Some videos reportedly reached millions of Facebook users in a country of fewer than 10 million inhabitants, while one non-advertised video attracted only 28,000 views. This contrast illustrates the role of paid promotion and the capacity of synthetic content to bypass political-ad filtering.

3. **Meta removed individual items without consistently disrupting campaigns.** Political Capital reported 1,739 items, comprising 1,110 profiles and 629 advertisements. Meta removed 82% of profiles and 61% of advertisements, an overall removal rate of 73%. Reviews generally took less than a day, but similar ads received inconsistent treatment. Removed advertisements were repeatedly republished, sometimes through replacement pages and multiple identifiers; at one point, 17 advertisements for the same video reportedly ran simultaneously. Across four monitored Facebook pages, repeated reuploads and replacement pages sustained a near-continuous presence for approximately 50 days, without clear evidence of systematic campaign-level escalation.
4. **Meta's handling of political and manipulated content was inconsistent.** Lakmusz reported 86 URLs: 50 political ads, 31 previously identified fake profiles and five pages, including two promoting Russia-linked fake news websites and three publishing realistic AI-generated videos without adequate labelling. Meta removed 66 URLs, but 19 political advertisements remained online, and action against AI-generated content was uneven. Ads with implicit electoral purposes were not always recognised as political, and the platform did not consistently apply its manipulated media policy.
5. **Google failed to act on reported political advertisements.** Political Capital reported 15 Google ads promoting the government's "National Petition" campaign. Google removed none and provided no written responses unless explicitly requested. Similar ads reported to Meta were removed. Google's unexplained classification and reclassification of political content further impeded independent assessment of its restrictions.
6. **Action against CIB and persistent fake profiles was insufficiently transparent.** Political Capital reported a network of 105 TikTok accounts identified in a CIB investigation by Context, the Romanian partner of FACT. TikTok said it had found no current violations, but provided insufficient information to establish whether the network had been investigated collectively. Lakmusz also identified 31 previously documented fake profiles that remained active. These cases suggest that individual-account review was not consistently accompanied by network-level investigation.
7. **Response times and transparency varied.** Meta generally processed reports within one day, but ordinary weekend reports were often reviewed only on Monday. During election weekend, responses frequently arrived within one to two hours. Across platforms, limited explanations of decisions and investigative procedures made it difficult to verify substantive reviews or assess repeat-offender enforcement.
8. **The main weakness was systemic rather than isolated.** Across Meta, Google and TikTok, responses to individual reports did not consistently address recurring campaigns, linked accounts or repeated circumvention. Limited advertising-library data further constrained independent verification and raised questions about the effectiveness of risk assessment and mitigation under Articles 34 and 35 DSA.

## 4.3 Recommendations for platforms

1. **Enforce political advertising restrictions consistently,** including indirect promotion, proxy organisations and electoral content whose purpose is apparent from its national context.
2. **Investigate advertisers and campaigns, not just individual ads.** Link reuploads, multiple identifiers and replacement pages, escalating repeated circumvention to advertiser- and account-level action.
3. **Strengthen AI-content detection and labelling,** applying consistent measures to synthetic political imagery and deepfakes under relevant advertising and manipulated-media policies.
4. **Improve advertising transparency.** Publish clear classification criteria and explain reclassification decisions, ensuring repositories allow researchers to identify mislabelled, removed and still-active ads.
5. **Investigate CIB at network level,** including previously identified accounts, and provide meaningful feedback on investigations and measures taken.
6. **Improve RRS response traceability.** Provide timely, reasoned decisions and maintain effective reporting and escalation throughout election periods, including weekends and election day.
7. **Assess cross-platform risks,** including connections between political advertising, coordinated accounts, affiliated pages and Russia-linked content distribution.
8. **Provide granular researcher access** to advertising and enforcement data, enabling analysis of reuploads, replacement campaigns and subsequent advertiser activity.

## 4.4 Recommendations for the DSA Election Guidelines

1. **Address systematic circumvention.** Risk mitigation should cover recurring campaigns, linked advertisers and pages, and repeated reuploads, not only individual advertisements.
2. **Clarify how indirect political promotion should be identified,** including implicit references, political logos, proxy organisations and national linguistic and political context.
3. **Set clear expectations for AI-generated electoral content,** including deepfakes in paid advertising and consistent application of labelling and other appropriate measures.
4. **Require advertiser- and network-level follow-up** for repeated violations, replacement pages and coordinated inauthentic behaviour.
5. **Improve enforcement accountability** through traceable RRS responses, meaningful explanations and evidence of how recurring patterns inform broader investigations.
6. **Promote consistent, continuous enforcement** across platforms, including during weekends and election day.

7. **Strengthen independent verification** through timely access to advertising libraries and granular enforcement data.
8. **Extend monitoring beyond official campaigns** to previously identified accounts, advertisers and influence networks, informing risk mitigation under Articles 34 and 35 DSA.

# 5. Bulgaria – Parliamentary Elections, April 2026 (BROD)

## 5.1 Context and monitoring activities

BROD monitored the elections amid cross-platform amplification, weak political advertising transparency, limited researcher access and insufficient Bulgarian-language moderation. Findings also draw on CSD research, DFRLab's March 2026 network analysis and BROD's MVI assessment of platforms' reporting under the Code of Conduct on Disinformation.

## 5.2 Main findings and platform shortcomings

1. **Enforcement depended heavily on user reports.** On Facebook and TikTok, violating content could circulate until individually reported, while policies were scattered across help sections and rarely displayed alongside content.
2. **Facebook group networks supported coordinated campaigns.** DFRLab documented a network using two pages, nine groups with over 211,600 members and six accounts to drive traffic to a fabricated, monetised news site. Group trading and repurposing also facilitated campaign activity.
3. **Political advertising restrictions encouraged less transparent channels.** Following Meta's announcement that it would stop accepting EU political, electoral and social-issue ads from October 2025, group networks continued operating without equivalent transparency, potentially shifting promotion to less attributable channels.
4. **AI-generated and sanctioned content remained accessible.** Deceptive AI-generated political content circulated on TikTok without adequate labelling. Russian state-media content appeared on TikTok and Facebook; TikTok's geo-blocking in Bulgaria left content visible in other Member States.
5. **Research datasets excluded substantial Bulgarian-language content.** Between 12 and 19 April 2026, 291 posts from 210 producers, each with at least 10,000 views, fell outside Meta Content Library. They generated at least 12.72 million views, with some reaching 200,000–800,000. The library's thresholds disproportionately limited visibility into smaller-language markets; during 30 March–5 April, fewer than one-third of over 7,000 matching posts were downloadable.

6. **Coordinated publishing targeted algorithms and reach.** The Bulgarian Pravda network published around 6,000 articles monthly, 96% during peak human activity hours, despite fewer than 1,500 average monthly visits. CSD assessed that it targeted search rankings and AI indexing. Facebook posts also used follower and top-fan tags, coordinated hashtags and links in comments to sustain reach.
7. **Telegram enabled cross-platform amplification outside the VLOP regime.** Analysis of 48,685 posts from 42 Bulgarian-language channels between 7 January and 31 March 2026 found that 56.2% belonged to cross-channel clusters. Monthly volume rose 75% from February to March, and clustered posts averaged 4,059 views versus 1,450 for others. Gateway outlets, aggregators and Facebook pages extended the reach of content from Telegram.
8. **Moderation and transparency remained inadequate.** Bulgarian-language moderation lacked sufficient staffing and cultural expertise. CSD also identified an inoperative trusted flagger programme, limited pre-election researcher access and gaps in country-level platform reporting.

## 5.3 Recent developments: autumn 2026 presidential campaign

1. **Crisis events activated established influence networks.** Preliminary CSD monitoring in October 2026 found that pro-Kremlin networks focused on geopolitical incidents and the Trump–Putin diesel deal rather than candidates or voting procedures. Narratives moved from Telegram to Facebook and mainstream debate within hours and were adopted by political actors.
2. **Comment-section mobilisation was difficult to assess.** Posts critical of Russia or supportive of the EU and Ukraine attracted hundreds of hostile comments within minutes. Without comment-level data, researchers could not establish coordination or assess enforcement consistency.

CSD welcomes comparative observations from other Hubs on event-driven activation, comment-section mobilisation and potential RRS reporting approaches.

## 5.4 Results of the MVI pilot and third evaluation report

BROD 2.0 developed the MVI framework to assess how very large online platforms and search engines report on the Code of Conduct on Disinformation. Each Service Level Indicator and Quantitative Reporting Element is scored 0-3 for Materiality (implementation), Verifiability (transparent methods and national/language breakdowns) and Impact (quantified outcomes). Where only EU-wide or global aggregates are provided despite expectations for national data, a Granularity Cap limits Verifiability and Impact to 1.

Commitments are divided into Tier 1 (demonetisation, political advertising and researcher empowerment) and Tier 2 (user transparency, user empowerment and fact-checkers).

The pilot assessed H1 2025 reports, published in September 2025, from Meta, Google Search, YouTube, TikTok and LinkedIn. Materiality was generally high, but Verifiability and Impact were frequently capped or scored zero. Bulgarian-specific figures were largely absent, confirming the lack of independently auditable national outcome data.

## 5.5 Recommendations for platforms

1. **Act proactively** rather than relying on individual user reports.
2. **Explain rules and remedies clearly,** including reporting procedures and expected outcomes, in line with applicable audiovisual media rules.
3. **Systematically detect and label AI-generated content.**
4. **Apply restrictions on sanctioned Russian media consistently across Member States.**
5. **Increase advertising transparency** and crack down on the buying, selling and repurposing of Facebook groups for coordinated campaign activity.
6. **Publish comparable national and language-level metrics**, including fact-checking outcomes, demonetisation, appeals and overturned decisions.
7. **Confirm Bulgarian-language moderation capacity** and publish election-specific mitigation and transparency reports.
8. **Adapt researcher-access thresholds** to smaller-language markets and high-reach civic content.
9. **Investigate networks and amplification infrastructure**, including coordinated behaviour and monetised link-sharing schemes.
10. **Assess cross-platform seeding**, including content originating on non-designated services; the Commission should continue monitoring Telegram's reported EU user numbers.
11. **Include crisis narratives adopted by political actors** in election risk assessments and crisis protocols.
12. **Provide timely researcher API access.** The Commission can request data directly under Article 40(1) DSA, with vetted applications processed through the relevant Digital Services Coordinator.
13. **Improve comment-level data access** for high-reach election content and report enforcement and appeal outcomes by Member State and language.

## 5.6 Recommendations for the DSA Election Guidelines

The Guidelines should address cross-platform amplification and crisis-related narratives, including content originating on non-designated services. They should also support timely researcher access, language-specific transparency and independently verifiable national enforcement outcomes.

# 6. Cyprus – Parliamentary Elections, May 2026 (MEDDMO)

## 6.1 Context and monitoring activities

Cyprus held parliamentary elections on 24 May 2026, after the TTPA took effect in October 2025. Meta and Google stopped accepting political advertising in the EU that month; TikTok has prohibited paid political ads worldwide since 2019.

MedDMO monitored Meta, Google and TikTok's transparency tools daily and submitted reports through the RRS. X was excluded because free researcher access had been withdrawn. Platforms engaged constructively in campaign meetings and removed almost every reported item, but underlying enforcement weaknesses persisted.

## 6.2 Main findings and platform shortcomings

1. **Political ads bypassed intake checks.** MedDMO identified nearly 2,500 election-related Meta ads running from October 2025. Advertisers could bypass political-content checks by answering “no”. About half were subsequently marked as removed, usually around two months after publication.
2. **TikTok's automated detection was ineffective.** Of nearly 900 paid political ads identified over seven months, automated systems removed only one. Following MedDMO's report and escalation through the Commission's Code of Conduct team, TikTok removed most adverts within a week, after much of their paid reach had already been delivered.
3. **Google's classifications obscured political content.** Although stricter identity checks limited political advertising, most videos from the one verified political advertiser identified by MedDMO were categorised as “Arts & Entertainment”.
4. **Anonymous political advertising persisted.** Five anonymous operations ran over 450 Facebook ads, mainly in the final campaign weeks. One page circulated fabricated opinion polls during a district-level polling blackout; Meta removed its ads only on the eve of the election, after up to approximately 120,000 impressions.
5. **Enforcement targeted ads rather than advertisers.** Removed ads were replaced the same day, and some operations created new pages after disabling. TikTok's broader sweep appeared to extend beyond individually reported accounts.
6. **RRS reporting tools were inadequate.** Meta lacked a dedicated political-ad category and did not retain reported links or reasons in its records. TikTok rejected links to its own ad library, while Google relied on email without case numbers.

7. **Campaign-time data access was insufficient.** Meta's spending data covered only ads classified as political; Google did not distinguish removed ads from expired ads; TikTok's API quota was quickly exhausted, and MedDMO's Research API access was approved only after the election.

## 6.3 Recommendations for platforms

1. **Verify advertisers before publication,** using official candidate lists and direct checks where necessary.
2. **Verify sponsor identity,** including for pages declaring no sponsor, and scrutinise new pages advertising in electoral districts shortly before voting.
3. **Apply advertiser-level measures for repeat violations,** including coordinated review of pages sharing names or replacing disabled pages.
4. **Improve RRS reporting tools** with political-ad categories, support for ad-library links, traceable case records, case numbers and bulk reporting.
5. **Improve advertising transparency.** Disclose spending for all active political ads during campaigns, distinguish removed from expired ads and retain removed ads for at least one year after elections.
6. **Adapt Article 40 DSA access to election timelines,** with campaign-time response deadlines, published API limits and temporary increases during elections.

## 6.4 Recommendations for the RRS and election coordination

The RRS improved response times, but effective action often depended on ad hoc escalation through the Commission. Regular platform meetings through polling day and a post-election debrief should become standard practice.

# 7. Malta – General Election, May 2026 (MEDDMO)

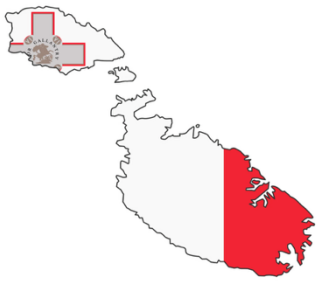
## 7.1 Context and monitoring activities

The snap election was called on 27 April 2026 for 30 May, about a year before the Labour administration's term was due to end. The Maltese MedDMO team therefore started using the RRS at short notice following coordination with colleagues monitoring Cyprus' election, as well as with the newly established EDMO Taskforce.

Monitoring focused on Facebook, Instagram and Google Ads. Platforms generally responded to reports filed through the RRS within one or two days, sometimes within hours, and removed most reported content. However, it is worth pointing out that platforms' responsiveness during the RRS period stands in stark contrast to their responsiveness (or lack thereof) outside of such a period. Regular users who have reported content that is clearly harmful (e.g. disinformation, harassment, etc.) usually wait a few weeks before getting a response, typically only to be told that no action has been taken against the content by the platform.

## 7.2 Main findings and platform shortcomings

1. **Delayed TikTok onboarding.** Access to its dedicated reporting platform was granted only during election week, because the platform was apparently experiencing issues when it came to onboarding due to the fact that the team was using a Gmail address for RRS purposes. This delay might have been avoided had guidelines, including information about accepted address types, been provided by platforms at the start of the RRS period.
2. **Political ads persisted despite restrictions.** Political advertising accounted for 290 of 296 flagged URLs (about 97%). The Google Ads Transparency Center, for example, listed hundreds of political ads categorised incorrectly under labels such as "Arts and Entertainment" and "Books and Publications".
3. **The advertiser's identity was not always disclosed.** Many adverts hosted by Google Ads appearing on popular Maltese websites did not identify their sponsors. This meant that the adverts could not be located in the Transparency Center, making it impossible to trace other adverts paid for by the same advertiser.
4. **Removed advertisements could be rapidly replaced due to poor platform moderation.** This was particularly the case of two advertisers: Clive Farrugia, from within the Office of the Prime Minister, and ONE Productions Ltd, the media company owned and operated by the governing Labour Party. Both advertisers were promoting the Labour Party campaign through Google Ads. They replaced adverts removed by Google almost immediately, and on a significant scale.



5. **Enforcement focused on individual ads rather than advertisers.** Despite repeated violations by identifiable political actors, platforms did not apply advertiser-level measures. This is essentially like fighting a hydra with a "whack-a-mole" approach, which drains resources that are better used elsewhere.
6. **A flagged profile associated with a covert influence operation was reinstated.** Three Facebook pages and related Instagram profiles, which appeared to be part of an operation to distort public discussion and galvanise political support in the run-up to the election, were reported to Meta through the RRS. Meta subsequently removed them from the platforms. However, one of the Instagram profiles appeared to have been reinstated shortly afterwards, once again highlighting a flaw in moderation practices. It is particularly concerning because the pages/profiles possessed clear signs of troll farming and questionable activity (read more on the influence operation here).

## 7.3 Recommendations for platforms

1. **Enforce political advertising restrictions at advertiser level.** Identify political actors – as their adverts are by nature political and in breach of platforms' own rules – as opposed to treating each ad separately.
2. **Improve moderation processes to detect political ads before they are allowed to run.**
3. **Improve advertiser transparency and traceability** so researchers can identify all ads associated with the same sponsor.
4. **Prevent circumvention through replacement ads** by improving moderation systems to identify political actors attempting to republish adverts in violation of platforms' own rules.
5. **Provide clear, timely RRS onboarding guidance**, including accepted email address types and technical requirements.

## 7.4 Recommendations for the RRS and election coordination

The RRS itself could be improved if platforms provide more comprehensive guidelines on their reporting tools, and address any queries about reporting procedures, from the start of the period. Furthermore, more time and energy could be directed towards tackling issues such as covert influence operations if platforms address shortcomings in their own procedures and approaches (for example, by shifting their focus to political advertisers as opposed to individual adverts, as described above).

Finally, platforms' responsiveness during the RRS exposed the gap between escalation channels available in the RRS period and ordinary reporting. Regular users (including our own team outside the RRS period) are usually met with silence or inadequate responses from platforms when reporting content that is clearly in violation of their standards. This highlights a serious flaw in platforms' moderation systems, which ultimately underscores most of the issues flagged during the RRS.

# 8. Conclusions

The six elections revealed recurring weaknesses in platforms' efforts to mitigate election-related disinformation, as well as systemic flaws in platforms' moderation practices. Across different national contexts, content-level interventions often failed to address the networks, advertisers and amplification mechanisms that sustain manipulation. Other common gaps concerned political advertising restrictions, AI-generated content, researcher access and cross-platform and cross-border coordination.

The revision of the DSA Election Guidelines should:

1. **Address coordinated manipulation and repeat offenders systematically.**

   Prioritise network-level investigations and follow-up monitoring of persistent inauthentic behaviour. Repeated violations should trigger broader investigation and sanctions, when the same actors or campaigns reappear through replacement accounts, new ads or alternative channels.

2. **Strengthen political advertising transparency and enforcement.**

   Identify direct and indirect political promotion consistently, including proxy organisations and content whose electoral purpose depends on national context. Improve sponsor identification, traceability and advertiser-level accountability, and ensure political content is not misclassified under unrelated categories.

3. **Extend risk mitigation beyond official campaigns and individual reports.**

   Address persistent influence networks, cross-platform amplification and crisis narratives before, during and after elections, including activity originating on non-designated services and subsequently adopted by political actors.

4. **Improve the detection and handling of AI-generated electoral content.**

   Strengthen measures against synthetic imagery and deepfakes, including paid promotion, and clarify expectations for labelling, removal and other appropriate interventions. Smaller-language markets require particular attention due to limited moderation capacity and linguistic expertise.

5. **Make the RRS earlier, more effective and accountable.**

   When possible, activate it sufficiently early to identify networks before they reach critical mass. Standardise reporting tools, escalation procedures and timely responses throughout election periods, with meaningful feedback on enforcement and recurring patterns.

6. **Strengthen researcher access and verifiable accountability.**

   Provide timely access to advertising, account, network and relevant comment-level data, subject to safeguards. Require granular, comparable outcomes disaggregated by Member State and language, enabling researchers to assess whether underlying

networks and amplification mechanisms were disrupted, not merely how many items were removed.

### 7. Enhance cross-border cooperation and safeguard independent monitoring.

Improve coordination among platforms, the Commission, Digital Services Coordinators and EDMO Hubs, including on networks spanning borders and services outside the VLOP regime. Protect researchers and fact-checkers from delegitimisation and undue pressure while maintaining the distinction between reporting potential violations and platforms' responsibility for enforcement.

**The overarching priority is a proactive, systemic and measurable approach to election-related risk mitigation.** Effective enforcement must address not only individual content but also repeated offenders, the advertisers, coordinated networks, synthetic content and amplification mechanisms that allow manipulation to persist and adapt.

The findings particularly demonstrate that formal restrictions are insufficient when filtering systems can be circumvented and repeated violations fail to trigger broader action. The Guidelines should therefore be assessed against demonstrable outcomes: whether platforms identify systemic risks, prevent repeated circumvention and reduce coordinated operations' capacity to manipulate the electoral information environment.

# 9. Original contributions

BROD - Romania

FACT - Moldova

HDMO - Hungary

BROD - Bulgaria

MedDMO - Cyprus

MedDMO - Malta

www.edmo.eu

The European Digital Media Observatory has received funding from the European Union under project number 300141274.