

# FIMI monitoring templates

PART 1 – INCIDENT QUALIFICATION

PART 2 – (SYSTEMIC) VIOLATIONS

PART 3 – COUNTER-MEASURES

The goal of this template is to improve the documentation of incidents and systemic risks by building a comprehensive, well-archived, date-tracked database, while developing structured incident reports that enable cross-country, event-based, and platform-specific comparisons for deeper analysis and trend identification.

**Disclaimer:** Using this template does not require any prior legal background. Where helpful, desk research and analytical support tools may be used to guide the process. However, such tools should be used cautiously, and outputs should be cross-checked and validated against reliable sources.

**FDEI**  
PROJECT

**FIMI**  
**-ISAC**



## Part 2 – (Systemic) violations

### A. INCIDENT ID

Conduct standard incident coding while placing particular emphasis on:

- **Incident creation and registration dates:** It is crucial to document both the date an incident occurs and the date it is registered, allowing researchers to measure the time lapse between incident creation and discovery.
- **Platform-specific reporting:** Ideally, separate reports should be generated for different platforms to better assess the Digital Services Act (DSA) and Code of Conduct (CoC) compliance more precisely. This approach ensures a clearer evaluation of platform-specific violations and regulatory obligations. If this is not possible, the researcher should clearly list the platforms on which the incident took place.

### B. TYPE OF INFRINGEMENT

#### **Preliminary check:**

The European Commission has opened multiple proceedings regarding potential infringements of the DSA. In order to help us identify any elements of **existing alleged infringements**, check if the incident is:

- Related to the spread of disinformation through a “verified” X account?
- Related to the absence of payment transparency on political ads on Facebook or TikTok?
- Related to the manipulation of recommender systems (algorithms) on TikTok?
- Related to the official complaint mechanisms efficiency on Meta and X?

→ Tip: Check [Digital Policy Alert](#) for a repository of digital policy measures

<p><b>Do you suspect that the incident may constitute an infringement?</b> If you replied yes, please specify which one</p>
<p><b>Content-related violation:</b></p> <ul style="list-style-type: none"><li>● Is the content harmful?</li><li>● Is the content illegal?</li></ul>
<p>If the content is allegedly illegal: Does the incident/campaign’s content constitute an infringement of (1) national legislation, (2) international legislation, or (3) a platform’s Terms of Service?</p>
<p><b>Behaviour-related violation:</b></p> <ul style="list-style-type: none"><li>● Is the behaviour/TTP harmful?</li><li>● Is the behaviour/TTP illegal?</li></ul>
<p>If the behaviour/TTP is illegal: Does the incident/campaign’s behaviour/TTP entail actions that constitute an infringement of (1) national legislation, (2) international legislation, or (3) a platform’s Terms of Service?</p>

**1) Type of violation – national legislation (illegal content or behaviour). According to you:**

- Does the incident/campaign violate existing laws against **disinformation** (including electoral disinformation)?
- Does the incident/campaign violate existing laws related to **impersonation** (e.g., copyright, trademarks, intellectual property, fraud, or online identity theft)?
- Does the incident/campaign violate existing laws regulating **foreign agents** operating in the country or engaging in covert political influence?
- Does the incident/campaign violate laws on **cybercrime** (e.g., hacking or malware distribution)?
- Does the incident/campaign violate existing laws on **hate speech**?
- Does the incident/campaign violate existing laws related to **terrorism** or **violent extremist ideologies**?
- Does the incident/campaign violate laws on **incitement to violence or public disorder** (including calls for harm against individuals, groups, or institutions)?
- Does the incident/campaign **violate consumer protection or unfair advertising laws** (e.g., false product claims, financial scams, or deceptive marketing practices)?
- Does the incident/campaign violate **data protection and privacy laws** (including unauthorised data collection, surveillance, or doxing)?

→ Note: This list is not intended to be exhaustive, but rather to raise awareness of the complexity and sophistication of FIMI campaigns, which often intertwine predominantly non-illegal patterns of behaviour with illegal activities spanning different areas.

If the answer to any of the questions listed under point 1) is yes:

- Describe the illegal content or behaviour
- Identify who is accountable for the violation: threat actor(s) (including amplifier(s)) or platform(s)
- If possible, identify the legal ground of the violation (based on personal knowledge)

**2) Type of violation – international legislation (illegal and harmful content and behaviour). According to you:**

- By allowing the incident/campaign, does the platform violate obligations under the **Digital Services Act (DSA)**, such as failure to mitigate systemic risks, ensure transparency, enforce content moderation policies, or remove illegal content as required?
- By allowing the incident/campaign, does the platform breach the **EU Code of Conduct on Disinformation (CoC)**, including failure to disclose political ads, inauthentic behaviour, coordinated manipulation, or non-compliance by platforms and advertisers?
- By allowing the incident/campaign, does the platform violate the **AI Act**, such as undisclosed synthetic media, deepfakes, algorithmic manipulation of public opinion, or failures in AI-driven content moderation?
- By sharing the incident/campaign, does the initiator/amplifier violate the **General Data Protection Regulation (GDPR)**, including unauthorised data collection, breaches of personal data rights, or unlawful profiling for political targeting?

→ (Extra since it is not binding:) By allowing the incident/campaign, does the incident/campaign fail to comply with relevant **European Commission guidelines on election security**?

If the answer to any of the questions listed under point 2) is yes:

- Describe the illegal or harmful content or behaviour
- Identify who is accountable for the violation: threat actor(s) (including amplifier(s)) or platform(s)
- Identify the legal ground of the violation

**3) Type of violation – platform’s Terms of Service (illegal and harmful content or behaviour). According to you:**

- Does the incident/campaign violate the **Terms of Service of the platform or any specific policy** (e.g., misinformation, coordinated inauthentic behaviour, hate speech, or unfair advertising)?

If the answer to any of the questions listed under 3) is yes:

- Describe the illegal or harmful content or behaviour
- Identify who is accountable for the violation: threat actor(s) (including amplifier(s)) or platform(s)
- Identify the contractual ground of the violation

## **C. SYSTEMIC INFRINGEMENT**

### **Systemic infringement as systemic failures in platform responses:**

- **Repetition of unaddressed incidents:** When the same type of incident occurs repeatedly without being accurately or consistently addressed, it signals a failure in the platform’s response mechanisms and enforcement policies.
- **Inaction despite awareness:** The platform, despite being aware of the risks, either chooses not to act or fails to implement effective mitigation measures, allowing harmful content or behaviour to persist.

### **Proving platform awareness and inaction:**

To demonstrate that a platform was aware of an issue but failed to act, consider the following evidence:

- **Reported content:** Incidents that were flagged through user reports, fact-checking organisations, or internal moderation tools but remained unaddressed.
- **Repetitive offences:** Recurring violations by the same accounts or networks, especially if prior enforcement actions (warnings, content takedowns, account suspensions) were taken but did not result in sustained corrective action.
- **Evidence repositories and prior knowledge:** Case study archives, incident databases, media coverage, investigative and transparency reports demonstrating that the platforms had prior knowledge of the incident but failed to act.

## **1. PLATFORM (IN)ACTION**

### **Flagging/reporting status:**

- Has the incident been reported/flagged?

If the answer is yes, please provide any reference or evidence. Additionally:

- Did the researcher (or someone known to the researcher) report/flag the incident publicly (identifying the asset publicly or in the media)?
- Did the researcher (or someone known to the researcher) report/flag the incident using reporting mechanisms of platforms?

→ Reminder: Unless the researcher reported/flagged the incident (or read about fact-checkers/other organisations flagging it), it is basically impossible to know if the incident was ever reported/flagged.

**Platform response (action v. inaction):**

- If the researcher (or someone known to the researcher) reported/flagged the incident, did the platform take action against the incident?

If the answer is yes:

- What action did the platform take against the incident?
  - Content labelled (e.g., misinformation warning, fact-check notice).
  - Content downranked (reduced visibility in recommendations).
  - Content removed (full deletion from the platform).
  - Account suspended (temporary or permanent action).
- When did the platform take action against the incident?
  - If possible, take note of the date of platform response(s) to measure the time lapse between the incident's first appearance and the platform's reaction.

## 2. REPETITION/RECURRENCE

**Incident recurrence:**

- Is the researcher aware of the same or similar incidents that occurred repeatedly on the same platform?

If the answer is yes, please provide a reference and, according to you:

- With what frequency did the same or similar incidents occur (e.g., multiple incidents occurring simultaneously or over a period of time)?
- Was the infringement previously known to the platform as a potential misuse (e.g., previous user reports or platform risk assessment reports)?

**Policy consistency in platform responses:**

- To the best of your knowledge, did the platform respond consistently across all cases?
  - No action was taken in any case.
  - Action was taken in some cases but not in others.
  - Same action was taken in all cases.
  - Different actions were taken in different cases.

If possible, take note of the date of platform response(s) to measure the time lapse between the incident's first appearance and the platform's reaction.

**Preventive measures against recurrence:**

- Did the platform implement any measures to prevent similar incidents from happening again (e.g., threat reports, policy updates, blocking domains belonging to a campaign, etc)?

If the answer is yes:

- Which measures?
- To the best of the researcher's knowledge, did they prove effective in reducing recurrence (please provide a reference)?

**FINAL ASSESSMENT:**

**Platform design and systemic risks:**

- Is there evidence that the infringement was caused by the design or functioning of the platform (e.g., algorithmic amplification, recommendation systems, lack of effective moderation tools)?

**Regulatory compliance:**

- Does the infringement constitute a violation of the platform's compliance obligations under the **DSA** (e.g., risk mitigation, transparency, content moderation enforcement)?
- If the platform adheres to it, does the infringement contradict the platform's commitments under the **EU Code of Conduct on Disinformation**?

If the answer is yes (and the platform adheres to the CoC)

- Has the platform fulfilled its obligations under the Code?

If the answer is no (and the platform does not adhere to the CoC)

- Has the platform proposed alternative mitigation measures to address the risks covered by the CoC?

→ Reminder: If aware of any other legal violations, the researcher should list them.

A large blue circle containing the text "EU DISINFO LAB" in white. The word "LAB" is enclosed in a white speech bubble shape. A black line extends from the top left of the circle towards the top left of the page.

EU DISINFO LAB

This template was created as part of EU DisinfoLab's contributions to the [FIMI-ISAC FIMI Defenders For Election Integrity \(FDEI\) project](#), an initiative that brought together 10 European organisations to collaboratively detect and respond to FIMI in electoral processes. The project aims to bolster democratic institutions by providing tools, establishing response teams, and creating an operational handbook.

A dark blue circle containing the text "FDEI PROJECT" in white. The "F" is stylized with a grid of dots. A black line extends from the top left of the circle towards the top left of the page.

FDEI  
PROJECT

A black circle containing the text "FIMI-ISAC" in white. To the left of the text is a logo consisting of three overlapping circles. A black line extends from the top right of the circle towards the top right of the page.

FIMI  
-ISAC