

A EUROPE THAT PROTECTS

The revised EU Crisis Protocol:
responding to terrorist content online



#EUprotects | May 2023

The EU Crisis Protocol (EUCP) provides a rapid cross-borders response to contain the viral spread of terrorist and violent extremist related content online. It was developed after the 2019 terrorist attack in Christchurch New Zealand and contributes to efforts undertaken at global level and in the context of the Christchurch Call for Action.

What is the EU Crisis Protocol?

The EU Crisis Protocol is a voluntary mechanism to help coordinate a rapid, collective and cross-border response to the viral spread of terrorist and violent extremist content online in response to real world incidents.

The Protocol:

- ✓ outlines the procedures, roles and responsibilities of key actors
- ✓ identifies the tools for monitoring and exchanging critical information
- ✓ ensures that any response safeguards fundamental rights
- ✓ respects relevant legal frameworks, in particular the General Data Protection Regulation

What is new?

The revised version of the EUCP integrates lessons learned:

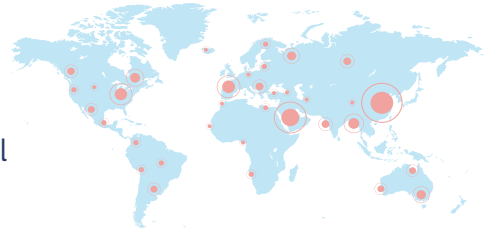
- ✓ clarifies the relationship between the voluntary EUCP and the Terrorist Content Online Regulation (TCO Regulation), in particular on Article 14(5) providing for an imminent threat to life situation
- ✓ simplifies activation criteria
- ✓ strengthens the protection of fundamental freedoms
- ✓ streamlines cooperation with international partners and other crisis response mechanisms
- ✓ provides guiding principles for crisis communication

Response mechanism: step by step



Step 1: Detection

Identification of an incident as a crisis. This includes an assessment of its geographical scope and potential for virality.



Step 2: Notification

Online service provider

- alerts Member States affected and/or Europol about a potential crisis.
- is alerted about a crisis involving its platform by Europol.

Member states

Member State and Europol alert online service providers via existing platforms and channels, as well as any third country affected about the crisis.

Points of Contact to be nominated by all the parties to the Protocol.



Step 3: Coordination and information sharing

Europol sets up a Crisis Coordination Team to support Member States, operational partners and Online Service Providers' response.

Voluntary exchange of information between law enforcement and online service providers on measures taken to remove and disable access to the extremist content online and effectively contain the crisis.

Preparation of operational plans by national law enforcement, real-time referrals to online platforms and sharing of hashtags, URLs and maintaining a crisis logs.

Safeguarding of Fundamental Freedoms by proportionate and targeted content moderation and preservation of content for judicial review and redress mechanisms



Step 4: Post-crisis report

A joint assessment of the response by all the actors directly involved to identify any gaps and lessons learnt for the future. Possible additional multi-stakeholder debrief with different actors to better understand adversarial tactics and the impact of crisis response while ensuring transparency towards the public.

Crisis communication principles

Throughout the crisis, EU Member States should communicate with the public, media and other relevant stakeholders on the viral spread of terrorist and violent extremist content online. In particular, they should provide factual information to:

- Reassure the public that the crisis is being managed
- Reduce the impact on vulnerable audience and ensure any tensions are mitigated
- Avoid that terrorists and extremists are using the attack to their advantage
- Prevent the spread of misinformation and disinformation