© Tech Against Terrorism

BRIEFING

European Regulation on Terrorist Content Online (TCO)

This new European Union rule, which came into effect last year, obliges hosting service providers offering their services in the EU to take active steps to remove terrorist content on their platforms.

This covers hosting service providers storing information offered by and at the request of a content provider and making this information available at the request of a content provider to a potentially unlimited number of persons. Hosting service providers include social media, video, image and audio-sharing services.

The providers have one hour to remove content once they receive a removal order by a competent national authority. These competent authorities include judicial, administrative, or law enforcement bodies appointed by EU Member States. The competent authorities designated by EU Member States are made public in an online register by the European Commission.

PLATFORMS AFFECTED

Hosting Service Providers (HSPs):

- As defined in point (b) of Article 1 of Directive (EU) 2015/1535 of the European Parliament and of the Council:
  - o Any Information Society service – "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services"
- Consisting of the storage of information provided by and at the request of a content provider
  - o I.e., that a user has provided information that is, or has been, stored and disseminated to the public by a HSP
- Hosts of public content: making information available to a potentially unlimited number of persons

Location of Platform: As per Article 2 of the TCO, HSPs that:

- Have a significant number of users of its services in one or more Member States; or
- Target their activities to one or more Member States

Size of Platform: The TCO applies to platforms of all sizes.

DEFINITION OF TERRORIST CONTENT

Terrorist content is content that:

- Incites the commission of one of the offences referred in (a) to (I) of EU Directive 2017/541, where glorifying terrorist material or advocating of terrorist offences (directly or indirectly), thus causing a danger of the offences being committed.
- Solicits a person to commit or contribute to a terrorist offence
- Solicits a person or a group to participate in activities of a terrorist group, as defined by Art.4 (b) of EU Directive 2017/541
- Provides instructions on the making of weapons for the purposes or committing or contributing to the committing of a terrorist offence.
- Constitutes a threat to committing a terrorist offence

Terrorist offence as defined in the EU Directive 2017/541, are the acts defined in Art 3. (criminal acts), with the aims of:

- Seriously intimidating a population
- Unduly compelling a gov or international org to perform or abstain from performing any act
- Seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation

Key Obligations

REMOVAL ORDERS (Section II, Article 3)

- **Competent Authorities have the power to issue removal orders to HSPs to remove content or disable its access in the EU**.
- HSPs should action the removal order **as soon as possible**, and in all instances **within one hour of receipt.**
- At least 12 hours prior to issuing the first order, the Competent Authority should provide the HSP with **applicable procedures and deadlines**.
- Removal orders will be used using the template form (Annex 1 of the TCO). They should include:
  - o A detailed explanation of why the content is considered terrorist (with a reference to the TCO definition)
  - o Information about redress available to both the HSP and the user
  - o Decision not to disclose removal order when necessary
- HSPs are to **inform Competent Authorities** of the content removal without undue delay, using the template in Annex 2, and specifying the time of the removal.
- **If a HSP cannot comply** – because of force majeure or other impossibility not attributable to the HSP, including technical and operational reasons – the HSP should inform the Competent Authority without undue delay using the template in Annex 3.
- **When the removal orders contain manifest errors, or lack sufficient information**, HSPs should inform the Competent Authority without undue delay.
- Removal orders are **final when the appeal deadline is reached without an appeal submitted, or when the decision has been confirmed by the appeal**.
- Issuing Competent Authorities should inform the HSP of a removal order; Residency Competent Authorities should inform the HSP when the removal order becomes final.
- If the issuing Competent Authority is not that of the HSP's residency, the issuing Competent Authority should submit a copy of the order to the residency Competent Authority.
  - o Residency Competent Authorities should scrutinise the removal order within 72 hours of receiving the copy to determine fundamental rights and freedoms infringement.
- Within 72 hours of receiving the removal order, HSPs and users have the **right to request a removal scrutiny** to the Competent Authority where the HSP has its establishment.
- If the removal order is adjudicated as a fundamental rights and freedom infringement, the HSP should immediately **reinstate the content**.

INFORMATION TO USERS / CONTENT PROVIDERS (Section III, Article 11)

- When a HSP removes or disables access to terrorist content, it must inform the user.
- Upon the user's request, the HSP should inform the user of the reasons for the removal or disabling, and their right to challenge the removal order, or provide the user with a copy of the removal order.
  - o Exception for instances where the Competent Authority issuing the removal order decides that it is necessary and proportionate that there be no disclosure for reasons of public security (e.g. the prevention, investigation, detection, and prosecution of terrorist offences) for as long as necessary, but not exceeding six weeks from that decision. In such cases, the HSP must not disclose any information on the removal or disabling of terrorist content.

© Tech Against Terrorism

PRESERVATION OF REMOVED CONTENT (Section II, Article 3)

- HSPs should **preserve all content removed** following an order or specific measure, as well as **any related data** removed as a consequence of the content removal.
  - Related data could include subscriber data, identity of the content provider, access data (date and time of the post, and of the log-in/off from the service), IP address.
- Preservation is necessary for:
  - Administrative or judicial review, or complaint handling
  - The prevention, detection, investigation and prosecution of terrorist offences
- Terrorist content and related data must be **preserved for six months** from the removal or disabling
  - The terrorist content must be preserved for a **further specified period** only if and for as long as necessary if requested by the Competent Authority or court
- When removing content through its own measures, a HSP must inform the Competent Authority if the content contains information about an **imminent threat to life or terrorist offence**.
- Preserved content can **only be accessed for the above specified purposes**.
  - HSPs must ensure that removed content and data are subject to appropriate technical and organisational safeguards.

USER APPEAL / COMPLAINT MECHANISM (Section III, Article 10)

- HSPs must **establish user-friendly complaint mechanisms,** and ensure that all complaints are dealt with **rapidly and in all transparency**.
- When removing content, HSPs should provide a **message in lieu** of the content to indicate the reason **why the content was removed** (including that it was removed in line with the TCO).
  - Should the Competent Authority find this message inappropriate or counterproductive, it should directly notify the HSP.
- Where content removal was **unjustified**, the HSP must r**einstate the content and notify the complainant** within two weeks of receipt.
- When **rejecting an appeal,** the HSP must **provide the user with an explainer**.
- Reinstatement of content or access thereto must not preclude administrative or judicial review proceedings challenging the decision of the HSP or the Competent Authority.

TRANSPARENCY (Section III, Article 7)

- In their Terms and Conditions, HSPs must clearly state their policy for countering terrorist content including (where appropriate) a meaningful explanation of the functioning of specific measures and use of automated tools.
- HSPs must publish a yearly transparency report about the actions taken regarding the identification and removal of terrorist content. The report must include:
  - Information about measures to identify and remove content
  - Information about measures to address the reappearance of content, in particular when using automated tools
  - The number of terrorist content removed or disabled in the EU following a removal order or specific measures, and the number of content not removed (when the order was dismissed)
  - The number and outcome of complaints handled by the HSP
  - The number and outcome of admin or judicial review proceedings requested by the HSP
  - The number of cases in which the HSP was required to reinstate content following a review
  - The number of cases in which the content was reinstated following a complaint from a user

© Tech Against Terrorism

SPECIFIC MEASURES (Section II, Article 5)

- HSPs **must use provisions to address the misuse of its services for the dissemination to the public of terrorist content**.
  - o HSPs must include the provisions in its Terms and Conditions.
- HSPs exposed to terrorist content must take **specific measures to protect** its services against the dissemination to the public of terrorist content.
- HSPs should act with due diligence and implement safeguards, including human oversight and verifications to avoid erroneous removal.
- **HSPs can decide on the measures**, which can include:
  - o Appropriate technical and operational measures, including appropriate staffing and technical means
  - o Ease of access and user-friendly reporting mechanisms
  - o Any mechanism to increase the awareness of the TCO on its services, including mechanisms for user moderation
  - o Any other measure to address the availability of terrorist content on its service
- Measures must meet the following requirements:
  - o Effective in mitigating the level of exposure of the HSP to terrorist content
  - o Targeted and proportionate, considering the technical and operation capabilities, financial strengths, number of users, and amount of content available on the service
  - o Applies in a manner fully accounting for fundamental rights, especially freedom of expression and information, privacy, and the protection of data
  - o Applied in a diligent and non-discriminatory manner
- Technical measures should have the appropriate safeguards, including human oversight and verification.
- HSPs **must report to the residency Competent Authority to determine the effectiveness and proportionality of the measures**, and whether the safeguards are sufficient.
  - o Reporting should first be done 3 months after receiving the Competent Authority decision that the HSP is exposed to terrorist content,[1] and then on a yearly basis
  - o When reviewing, the Competent Authority will consider different elements, including the size of the platform and its user base in the EU
  - o If the Competent Authority deems the measures to be insufficient, it can require the adoption of specific measures. These cannot lead to a general monitoring obligation, obligations to actively seek facts or circumstances indicating illegal activity, or obligations to use automated tools.

APPEAL PROCESS FOR HSPS (Section III, Article 9)

- HSPs have the **right to challenge removal orders,** or any decisions resulting from the review of a removal order.
- Removal orders can be challenged in the courts of the Member State of the issuing Competent Authority.
- HSPs can challenge decisions related to specific measures or related penalties.

1. A HSP is considered exposed if the Competent Authority of its residency finds it so – including if the HSP has received 2+ final removal orders within 12 months – and notified the HSP of its decision.

© Tech Against Terrorism

CRISIS SITUATION / THREAT TO LIFE (Section IV, Article 13)

- HSPs must **"promptly" inform the relevant authorities** of the Member State concerned, or the Competent Authority of the Member State they are established in / have a legal representative in, of **imminent threat to life or a suspected terrorist offence**.
  - This is limited to "terrorist offence" as defined in Article 3(1) of EU Directive 2017/541.
  - This does not imply a requirement to actively seek evidence.
- In case of any doubt over the Member State concerned, the HSP should contact Europol.

LEGAL PRESENCE IN THE EU

- There is **no physical presence** mandate to the TCO.
- HSPs fall under the jurisdiction of the Member State where they have their main establishment or where their legal representative is established.
- For HSPs which do not have the above, then any Member State has jurisdiction and can impose penalties (in respect of the ne bis in idem principle – no double prosecution or penalties).

PENALTIES (Section VI, Article 18)

- Member States are responsible for adopting rules and penalties (administrative or criminal nature), as well as financing guidelines for non-compliance (including systematic or persistent failure to comply).
- Penalties can take different forms, from **formal warnings to fines**.
- HSPs can face severe penalties if they **systematically or persistently fail to remove content within one hour of receipt** of the removal order (up to 4% of the global turnover for the preceding business year).
- Financial penalties will account for the HSPs financial resources.
- Competent Authorities must consider if the HSP is a start-up, micro-, small-, or medium-sized enterprise as defined in Commission Recommendation 2003/361/EC.
  - They should also consider other information, such as negligence or intention.
- Penalties must not encourage the removal of non-TCO material.

COMPETENT AUTHORITIES (Section IV)

- Competent Authorities are appointed by Member States and are to be publicly listed.
- Competent Authorities should coordinate and cooperate on removal orders, special measures, and penalties.
  - Two Competent Authorities should not issue the same removal order.
- Competent Authorities should exchange information and coordinate as appropriate with Europol before issuing removal orders. Europol is to provide support in line with its mandate and existing legal framework.
- Member States are encouraged to make use of the existing tools developed by Europol, including the Referral management app.
- Member States responsible for issuing penalties should be informed of all removal orders issued and exchanges between the platforms and other Competent Authorities.
- Referrals based on a platform's voluntary consideration per its Content Standards should remain available in addition to removal orders. The TCO does not preclude Europol from using voluntary referrals as a means to address terrorist content.

© Tech Against Terrorism

ENABLING TECH COMPANIES TACKLE TERRORIST CONTENT ONLINE IN EUROPE

Tech Against Terrorism Europe aims to help smaller hosting service providers (HSPs) disrupt terrorist content online whilst respecting human rights and fundamental freedoms.

This project will drive greater awareness of the EU's terrorist content online (TCO) regulation, supporting smaller tech companies in meeting the requirements to counter the terrorist threat.

POWERED BY TECH AGAINST TERRORISM

Tech Against Terrorism is an independent public-private partnership initiated by the United Nations Security Council. We will scale up Tech Against Terrorism's expertise, network, and technologies to drive greater awareness of the EU's TCO regulations.

The European initiative will augment Tech Against Terrorism's existing mentorship programme, enabling tech companies improve their internal processes, policies and technologies to better combat terrorist use of their services.

Capacity Building Programme

Drawing from Tech Against Terrorism's mentorship expertise, Tech Against Terrorism will give bespoke support to European hosting service providers, helping them to establish the necessary internal mechanisms to adhere to European regulation on terrorist content (TCO).

Knowledge Sharing Platform

Our carefully-curated policy resource will be expanded to cover European regulation on terrorist content.

We will also be creating additional new resources and updating existing ones to continue sharing cutting-edge key insights and policy best practice.

Terrorist Content Analytics Platform

We aim to support the European tech sector in identifying and alerting terrorist content in scope of the TCO.

We recommend content flagged under the TCO regulation be removed or geoblocked in the EU.

IN PARTNERSHIP WITH A EUROPEAN-WIDE NETWORK OF EXPERTS

The project will be coordinated and delivered by Tech Against Terrorism and SAHER Europe, a security and research consultancy. To sustain this effort, Tech Against Terrorism Europe will bring together a consortium of partners from academia and civil society. Members of the consortium include: Dublin City University, JOS Project, Ghent University, Ludwig Maximilian University of Munich and Swansea University.

FUNDED BY THE EUROPEAN UNION

The Tech Against Terrorism Europe project is funded by the European Union (ISF-2021-AG-TCO-101080101). This project will support smaller hosting services providers (HSPs) in building their counterterrorism frameworks and with transparency reporting, as required by the EU's terrorist content online (TCO) regulation and in Directive (EU) 2017/541.