ALLIES

THE TCO REGULATION

In April 2021, the European Union introduced the TCO Regulation, a critical step in addressing the rising threat of terrorist content online. This regulation, which came into effect on June 7, 2022, aims to curb the dissemination of terrorist content on digital platforms.

It is designed to complement existing legal frameworks governing online content within the EU, but its unique focus is on preventing the spread of extremist material that can incite violence and contribute to radicalisation.

What is the TCO Regulation?

- Origins of the TCO Regulation
- Scope of Application
- Key Elements
- Alignment with Key EU Counter-Terrorism and Security Policies

What is Radicalisation?

- Radicalisation in the Digital Age

What is Terrorist Content?

ALLIES Reporting Template

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

Origins of the TCO Regulation

In response to the 9/11 attacks, the United Nations swiftly adopted measures to combat terrorism, including financial restrictions and legal definitions of terrorist acts. The **2001 Budapest Convention on Cybercrime** and the **2005 Convention on the Prevention of Terrorism** addressed cyber threats and public provocation to terrorism at European Level. Building on these, the EU adopted **2017 Directive (EU) 2017/541** establishing a framework for removing terrorist content online, paving the way for the TCO Regulation.

What is Radicalisation?

The European Commission defines radicalisation as a "phased and complex process in which an individual or a group embraces a radical ideology or belief that accepts, uses or condones violence, including acts of terrorism, to reach a specific political or ideological purpose." This process can be influenced by a range of personal, political, and social factors that drive individuals or groups toward extreme ideologies that justify or glorify violence, including terrorism.

Radicalisation in the Digital Age

The internet has transformed radicalisation by enabling extremist ideologies to spread more rapidly and extensively than before. Online platforms allow isolated individuals to connect, share extremist views, and reinforce radical beliefs, making it easier for such ideologies to gain influence. Unlike traditional forms of radicalisation that occurred in physical spaces, the digital environment allows for the immediate and global dissemination of extremist content.

What is Terrorist Content?

The TCO Regulation defines "terrorist content" as **any material (including text, audio, or video) that incites terrorist offenses, glorifies terrorist acts, provides instructions for creating or using weapons for terrorist purposes, or promotes terrorist groups or recruitment/participation**. However, the regulation exempts content intended for education, journalism, artistic expression, research, or raising awareness about terrorism. As part of the ALLIES training we may showcase some terrorist content as example. This exception ensures a balance between safeguarding public safety and protecting freedom of expression.

What is the TCO Regulation?

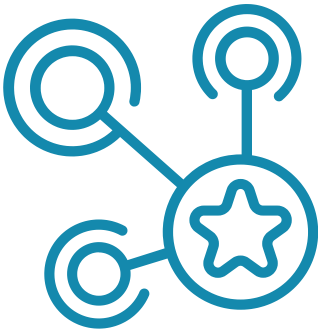
The TCO Regulation (EU 2021/784) focuses on ensuring that terrorist content is swiftly detected and removed from online platforms, preventing its further dissemination and impact. It requires hosting service providers (HSPs) to remove or disable access to such content within one hour of receiving a removal order issued by a competent authority. The regulation emphasizes the need for close cooperation between authorities and HSPs to ensure rapid action, while promoting transparency through annual reporting from both sides. It also fosters cross-border collaboration, aiming for a unified approach to addressing terrorist content across the EU.

Who does the TCO Regulation apply to?

The TCO Regulation applies to **Hosting Service Providers (HSPs) offering services within the EU, regardless of their primary location**. These are:

- Hosting service providers operating in the EU or offering services in the EU (e.g. webhosting service providers)
- Platforms like social media, video-sharing, image-sharing, and audio-sharing services
- Websites and platforms that store and share user-generated content (e.g. imageboards)

What are the key elements of the TCO Regulation?



- **Swift removal obligation**: HSPs must remove terrorist content within one hour of receiving an order from authorities.
- **Removal orders**: National authorities can issue removal orders to HSPs to take down terrorist content.
- **Transparency and Reporting Obligations**: HSPs are required to publish annual reports detailing actions on terrorist content, including removals, complaints, and reinstated content. National authorities are also required to publish annual reports on removal orders, their implementation, outcomes of complaints, and penalties.
- **Penalties for Non-Compliance**: HSPs that fail to adhere to the regulation may face substantial fines, serving as a deterrent for non-compliance.
- **Information to Content Providers**: HSPs must inform content providers when their content is removed or access is disabled and, upon request, provide the reasons or a copy of the removal order.

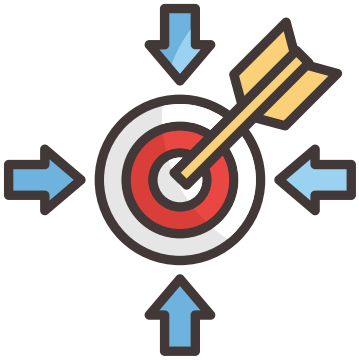
What are the key elements of the TCO Regulation?

- **Complaints Mechanisms**: HSPs are required to establish an accessible mechanism for content providers to submit complaints if their content is removed or access is disabled, and must review complaints quickly, informing the complainant of the outcome within two weeks. If a complaint is rejected, the provider has to explain the reasons, but the complainant can still pursue administrative or judicial review.
- **Legal Remedies for Content Providers and HSPs**: HSPs and content providers whose content is removed have the right to challenge removal orders or decisions before the courts of the Member State that issued the order or made the decision.
- **Cooperation and Information Sharing**: HSPs are encouraged to cooperate with national authorities, law enforcement agencies, and other relevant entities, facilitating information exchange to effectively tackle the spread of terrorist content across platforms.
- **Protection of Fundamental Rights**: Measures to remove terrorist content must respect freedom of expression and other rights.
- **Proactivity**: HSPs are encouraged to proactively identify and remove terrorist content.

Alignment with Key EU Counter-Terrorism and Security Policies

The TCO Regulation is closely aligned with several key EU documents that shape the Union's approach to counter-terrorism and security. It complements **the Directive on Combating Terrorism**, which strengthens measures against terrorist offenses, including penalties for participation in terrorist organizations and acts of terrorism. While the Directive broadly addresses terrorist actions, the TCO Regulation specifically targets the digital aspect by focusing on the online dissemination of terrorist content. It complements the Directive's objectives by tackling how the internet is used to incite violence, promote terrorist ideologies, and facilitate recruitment, reinforcing these efforts in the digital realm. A key measure of the regulation is the one-hour removal rule, which requires Hosting Service Providers (HSPs) to swiftly **remove terrorist content within one hour of receiving an order** from national authorities. This urgent timeframe ensures real-time disruption of online terrorism, directly supporting the Directive's broader goals of preventing and countering terrorist activities.

The TCO Regulation also supports **the EU Counter-Terrorism Agenda**, which outlines the EU's strategic approach to preventing, anticipating, protecting against, and responding to terrorism. The regulation addresses the growing challenge of terrorist content online, as identified in the Agenda, by imposing **transparency reporting obligations** on HSPs. These reports require platforms to regularly (on a yearly basis) disclose their actions to remove terrorist content, providing valuable insight into the effectiveness of their measures. This transparency supports the Agenda's goals of preventing radicalisation by holding HSPs accountable for content moderation and encouraging continuous improvement of their practices.



Additionally, the TCO Regulation aligns with **the EU Security Union Strategy**, which aims to enhance the EU's resilience to security threats. One of the regulation's key measures that complement the Strategy is the obligation for **cooperation between HSPs and Member States**. This ensures platforms work closely with national authorities to detect, remove, and prevent terrorist content from reappearing. By fostering collaboration, the regulation strengthens the Strategy's goal of improving collective security against digital threats.

The TCO Regulation also operates alongside **the Digital Services Act (DSA)**, which sets general rules for tackling illegal content online. While the DSA addresses broader illegal content, the TCO Regulation targets terrorist content specifically by providing a **faster response time** than the general obligations set forth in the DSA. Additionally, the TCO Regulation introduces strict risk assessment and mitigation measures, requiring HSPs to evaluate and address the risks associated with terrorist content on their platforms. These measures ensure platforms proactively prevent the dissemination of terrorist material.

Finally, the TCO Regulation respects the **Charter of Fundamental Rights of the European Union**, ensuring that measures to remove terrorist content do not infringe upon fundamental rights, particularly the freedom of expression. It ensures that any removal requests are accompanied by safeguards, such as the right to appeal. These protections, combined with the regulation's transparency obligations, ensure that **content removal is accountable, transparent, and consistent with the Charter's protections.**

ALLIES Reporting Template

The first section captures essential details about the HSP, including the name of the provider or its legal representative, the country of establishment, and contact information for regulatory purposes. This helps ensure clear accountability and communication channels between the HSP and the authorities.

The template then moves on to the identification of terrorist content, asking HSPs to classify the content based on specific criteria, such as whether it incites, solicits, or glorifies terrorist acts, provides instructions for committing terrorist offences, or constitutes a threat to commit such acts. It also prompts HSPs to describe the method through which the content was identified, whether through automated tools, employee flagging, user reporting, or other means. The hosting service providers are then asked to specify the actions taken to address the identified content, such as removal or disabling access, and whether the content provider was notified of these actions.

ALLIES Reporting Template

If you have identified suspicious content that may be considered as terrorist being hosted via your services, you can report it voluntarily to the competent national authority where your company has its main establishment or where your legal representative resides. Please note that you are under no obligation to report terrorist content that you have identified yourself, but you can use this first part of the template as a good practice and to seek further advice from the authorities in case of doubt whether the removal or disabling of the contents was legitimate.

REPORT FOR IDENTIFICATION OF TERRORIST CONTENT ONLINE

Name of the Hosting service provider (HSP) [or] Name of the legal representative of the HSP
Name

Member State of the EU of main establishment of the HSP [or] Member State of the EU of residence or establishment of the legal representative of the HSP
Member State

Contact point for the purpose of Regulation (EU) 2021/784 (TCO Regulation)
Name
E-mail address

The content published within our services has been deemed as potentially terrorist in nature on the following basis [Select all that apply]:

- ☐ incites others to commit terrorist offences (e.g., by glorifying terrorist acts; by advocating the commission of such acts)
- ☐ solicits others to commit or to contribute to the commission of terrorist offences
- ☐ solicits others to participate in the activities of a terrorist group
- ☐ gives instructions on making or using explosives, firearms, or other dangerous items, or on methods for committing terrorist acts
- ☐ constitutes a threat to commit one of the above offences
- ☐ Other: ...

ALLIES Reporting Template

REPORT FOR IDENTIFICATION OF TERRORIST CONTENT ONLINE

The suspicious content has been identified via:

- ☐ automated tool for identifying terrorist content implemented at my organisation for internal monitoring of our services;
- ☐ flagging by employee(s) as a result of manual screening;
- ☐ flagging by users of our services;
- ☐ Other: ...

The suspicious content has been:

- ☐ removed;
- ☐ access to it has been temporarily disabled in all Member States;
- ☐ Other: ...

The content provider has been informed of the removal of/ disabling access to their contents:

- ☐ Yes
- ☐ No
- ☐ Other: ...