FRISCO

Fighting Terrorist Content Online

FRISCO INSIGHTS

The EU Regulation on Terrorist Content Online: are European platforms ready?

In 2023, the FRISCO Team conducted a study (available in full-length here) to assess the readiness of small European online platforms (i.e. 'Hosting Service Providers') regarding the provisions of the EU Regulation on Terrorist Content Online. We gathered their insights and identified the most common challenges they face. In this article series, we offer a comprehensive breakdown of our findings. In this third and final article, we will present our main results and answer our research question: are small European platforms ready to cope with the TCO Regulation (3/3)?

Our mapping report is the result of an investigation conducted over a six-month period ending in May 2023, mixing primary and secondary research techniques (i.e., semi-structured interviews, online survey, secondary research). The results of our secondary research were presented in the first two articles in this series. We will now focus on the key findings of our primary research, thus answering our main question: are small platforms ready for the TCO Regulation? During this primary research, we gathered the feedback of more than 50 European Hosting Service Providers (HSPs) and relevant stakeholders. The findings stemming from this exercise, the first of their kind to our knowledge, were recently highlighted in a European Commission report published on the 14th of February 2024[1]. Given the public interest in our work, we decided to present and summarise our findings here, in this series.

A very limited awareness

Micro and small HSPs have a very limited awareness and knowledge of the TCO Regulation.

On a scale of 1 to 5 (1 = Not Aware; 5 = Highly Aware), 42.4% of the respondents to our questionnaire were not familiar at all with the TCO Regulation and the remaining 48.5% had only a partial knowledge of what it entailed in general and for their company. Only 9,1% considered having an awareness of 4. As a comparison, we found that these HSPs were clearly more aware of the Digital Services Act (DSA), with 57,6% being partially aware and 9,1% being highly aware (i.e., reaching 5).

A perceived absence of risk

Most micro and small HSPs perceive themselves at low risk of being exposed to terrorist content.

[1] Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online. Available here.

However, despite this evident lack of awareness and preparedness, a large majority of HSPs perceived themselves to be at low risk of being exposed to terrorist content (i.e., having their services misused by terrorists). On a scale of 1 to 5 (1 = Very Unlikely; 5 = Very Likely), 72,7% of the respondents considered that their services run a low risk of exposure to terrorist content. 51.5% even considered that their platforms were at the lowest possible risk of exposure (i.e., 1). These HSPs find themselves in what we have termed a 'reactive posture', which means that they will only consider taking action, and, consequently, complying with EU Regulations, if they are obliged to do so.

A lack of tools and processes

Micro and small HSPs lack the tools and formal processes to comply with EU Regulations.

Our third finding is that most of the small-scale HSPs surveyed are currently missing the core infrastructure to identify, monitor and remove terrorist content. Most of them do not even moderate user-generated content (57,6% of the respondents) or do so only partially (21,2% of the respondents). Therefore, measures required by the TCO Regulation, such as complaint mechanisms, automated classifiers, points of contact or transparency reports, were only rarely implemented by the HSPs surveyed. The resources they are currently lacking to build the appropriate processes (i.e., to identify and remove terrorist content, and comply with EU Regulations) are diverse:

- *Technical resources*: tools for automated detection, monitoring, or content moderation.
- *Human and legal resources*: dedicated staff for content moderation and legal issues (e.g. monitoring the legal framework).
- *Financial resources*: funds to buy tools, hire new staff, monitor regulations, etc.

The general lack of resources of micro and small HSPs clearly affects their ability and willingness to invest in developing the right processes and implementing efficient tools, not only to be compliant with EU Regulations but also to serve their own business needs. As said prior, most intended to postpone the investment in technical, human, and legal resources for as long as possible.

A need for legal and technical support

Micro and small HSPs need legal information and technical support.

Finally, the large majority of HSPs expressed the same needs: gaining familiarity with the TCO Regulation and getting access and guidance to tools for content moderation. 81,8% of the respondents stated they needed help to understand the TCO Regulation and comply with its provisions. Respectively 66,7% and 63,6% of the respondents, expressed their need for access to and advice on content moderation tools and automated content identification tools.

European platforms are not ready

As a result of our investigation, it became clear that there is a very significant gap between the processes currently being implemented by European HSPs and those they actually need to implement to comply with the provisions of the TCO Regulation. In addition, and more worryingly, this gap between *what is being done* and *what should be done* was confirmed in most of the areas we investigated, not to mention the lack of awareness and the distorted risk perception we witnessed. At the moment, most micro and small European HSPs are not ready to comply with the TCO Regulation and need all-round support, both for legal and technical issues. They must be equipped swiftly with the appropriate information, resources, and capacities to remain as impervious as possible to malicious actors, tackle the exploitation of their services and comply with EU Regulations to steer clear of potential fines. It is crucial to incentivise micro and small European HSPs to be proactive and comprehensive in the efforts they carry out to protect their services from harmful content.

What's next?

The mapping report was a pivotal step for the FRISCO project, enabling us to adapt the resources and services we offer to European HSPs. The first-hand information gathered during our investigation forms the very basis on which we deploy our activities (e.g., tools, frameworks, training modules, best practices documents, etc.). First and foremost, our team has developed and introduced a set of three tools. The first two tools, a self-assessment questionnaire and an interactive process map, dwell upon the TCO Regulation's provisions and specificities and have been designed to help HSPs assess their compliance and refine it. The third, a content moderation tool based on Tremau's in-house solution, will provide them with a practical and operational framework for dealing with harmful content. Beyond these tools, the FRISCO project is also offering online training courses, producing best practices materials, and undertaking extensive research on related topics.

Our objective is to offer actionable solutions to help HSPs build robust processes and policies, while complying with the TCO Regulation. With this comprehensive approach, we are helping to remedy the current lack of information and preparation that has left many HSPs unaware of both their duties and how to fulfil them. Ultimately, we wish to contribute to the creation of a safer digital environment.

Adeline KUGLER

Pierre SIVIGNON

FR!SCO

Fighting Terrorist Content Online

About FRISCO

FRISCO ("Fighting Terrorist Content Online") is an EU-funded project implemented by a team of 7 partners across Europe. Our main objective is to raise awareness among small tech companies and online platforms and to help them comply with the EU Regulation on Terrorist Content Online (TCO). By supporting the fight against terrorist content in Europe, we are helping to prevent and counter violent extremism online and to create a safer online environment.