



## D4.2: Tools and approaches for small HSPs to address TCO

<b>Grant Agreement ID</b>	101080100	<b>Acronym</b>	FRISCO
<b>Project Title</b>	Fighting teRrorISt Content Online		
<b>Start Date</b>	15/11/2022	<b>Duration</b>	24 Months
<b>Project URL</b>	<a href="https://friscoproject.eu">https://friscoproject.eu</a>		
<b>Contractual due date</b>	14/05/2024	<b>Actual submission date</b>	31/05/2024
<b>Nature</b>	R	<b>Dissemination Level</b>	PU
<b>Author(s)</b>	Adeline Kugler (Tremau)		
<b>Contributor(s)</b>	Isabelle Arnson (Tremau), Pal Boza (Tremau)		
<b>Reviewer(s)</b>	Rositsa Dzhekova (VPN)		



This project has received funding from the European Union's Internal Security Fund (ISF) programme under Grant Agreement No 101080100. Views and opinions expressed are 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.

**Document Revision History (including peer reviewing & quality control)**

Version	Date	Changes	Contributor(s)
v1.0	06/05/24	First Version	Tremau
v1.5	10/05/24	Quality Control	VPN
v2.0	15/05/24	Final Version	Tremau

## Executive Summary

The Fighting Terrorist Content Online (FRISCO) project is funded by the European Commission – Internal Security Fund and is in the process of being implemented by 8 partners from 6 different EU Member States between 2022 and 2024. FRISCO aims to support Hosting Service Providers (HSPs) to address the dissemination of terrorist content online. The Regulation (EU) 2021/784, addressing the dissemination of terrorist content online (TCO Regulation), entered into force in this context on the 7th of June 2021 and is applicable as of the 7th of June 2022. It sets out several specific measures that HSPs must implement to address the misuse of their services. The FRISCO project aims to help HSPs comply with the TCO regulation through tailored training, compliance tools and best practice guidelines.

This brochure provides an overview of the technical tools and solutions available to HSPs, presented into the following main categories:

- TCO Regulation compliance tools developed under FRISCO
- Content moderation software
- Tools for detection of harmful/illegal content
- Hash-matching tools

It is based on an online marketplace held by the FRISCO project on 18-19 April, aimed at familiarising HSPs with various solutions providers that can support with addressing the dissemination of terrorist content online and increase compliance with the TCO.

This brochure is designed to equip HSPs with a comprehensive list of technical solutions. These tools are aimed at facilitating full compliance with the TCO regulation. The solutions are offered by a diverse range of service providers, each focusing on various software-based measures to address terrorist and other harmful online content. These range from specific detection tools to all-inclusive content moderation software and advanced hash-matching tools.

This brochure aims to foster collaboration among various stakeholders from the TCO sphere. It encourages the creation of synergies and promotes the sharing of experiences, ultimately contributing to a safer digital environment for everyone.

## Table of Contents

1 Introduction	6
2 Purpose and Scope	6
3 Approach for Work Package and Relation to other Work Packages and Deliverables	8
3.1 Methodology and Structure of the Deliverable	8
4 FRISCO tools	10
Self-assessment questionnaire	10
Process map	10
5 Content moderation software	11
FRISCO Content moderation tool - Tremau - France	11
Utopia Analytics - Finland	11
Bodyguard - France	12
6 Detection tools	13
Sightengine - France	13
Textgain - Belgium	13
Identrics - Bulgaria	14
Logically AI inc. - UK	15
ALLIES project	16
7 Hash-matching tools	17
Web-IQ - Netherlands	17
Tech Against Terrorism	17
8 Final insights	19

## List of Terms & Abbreviations

Abbreviation	Definition
HSP	Hosting Service Provider
TCO	Terrorist Content Online
NLP	Natural Language Processing
AI	Artificial Intelligence

## 1 Introduction

In the digital landscape, where every interaction matters, the internet has unfortunately become a space where negativity and extremist ideas thrive. In response to these challenges, the EU took a significant step by introducing the Digital Services Act (DSA) fully applicable since February 2024. This landmark legislation aims to combat hate speech and disinformation online, promoting a safer digital space. Additionally, the EU has adopted a targeted Regulation on Terrorist Content Online (TCO) in April 2021 to address violent extremism and the dissemination of such content, setting out specific measures that Hosting Service Providers (HSPs) exposed to TCO must implement, results in HSPs, especially small and medium ones facing unique challenges in implementing TCO measures.

This is where the FRISCO project steps in, aiming to not only alleviate the burden on providers but also to create a collaborative ecosystem. Our goal is to foster partnerships and networking opportunities among micro and small HSPs, multiplier associations, industry experts, and state and international stakeholders.

## 2 Purpose and Scope

FRISCO ("[Fighting teRrorISt Content Online](#)") is an EU-funded project whose main objective is to raise awareness among small online platforms ("Hosting Service Providers") and to help them comply with the EU Regulation (number) on Terrorist Content Online ("[TCO Regulation](#)"). By supporting the fight against terrorist content in Europe, we are helping to prevent and counter the spread of violent extremism and to create a safer online environment.

### FRISCO IN A NUTSHELL

#### An EU-Funded project (2022-2024)...

- Implemented by a team of [8 partners](#)<sup>1</sup>
- Funded by the Internal Security Fund<sup>2</sup>
- With a total budget of €1,536,637

#### ...to support Hosting Service Providers<sup>3</sup>

- Support HSPs in their compliance and content moderation efforts
- Alleviate their operational burdens relating to the TCO Regulation
- Foster multi-stakeholders collaboration and partnerships

<sup>1</sup> NCSR-Demokritos, Violence Prevention Network, Tremau, French Ministry of the Interior, Civipol, D-Learn, IVSZ, INACH

<sup>2</sup> ISF-2021-AG-TCO

<sup>3</sup> All online platforms storing information provided by and at the request of a user in the EU - i.e., with user-generated content publicly available.

### TCO REGULATION NEW MEASURES

The TCO Regulation aims to disrupt terrorist content on the Internet and sets out new obligations for HSPs offering their services in the European Union:

- **Terrorist content** is defined as text, images, audios or videos used to incite terrorist acts, give instructions on how to commit offences or solicit participation in terrorist groupso
- **Golden hour rule:** once HSPs have received a "removal order" from a [competent authority](#), they have one hour to remove the flagged content.

- **Potential fines:** HSPs that do not systematically comply with the rules are liable to be fined up to 4% of their global turnover.

### FRISCO OBJECTIVES

In consequence, our main objective is to raise awareness among micro and small HSPs, foster their compliance with the TCO Regulation, and help them protect their services against terrorist content. We support them through:

- **Awareness raising** - we inform HSPs about their new obligations.
- **Tools production** - we develop tools, frameworks and mechanisms for them.
- **Knowledge-sharing** - we share information, experiences and best practices.

### FRISCO ACTIVITIES

Our team will produce three main types of resources to support HSPs:

- A **Toolbox:** a [self-assessment questionnaire](#), a [process map](#) and a [content moderation tool](#).
- A **Training Programme:** seven training modules accessible via an online platform.
- **Best practices materials:** a manual, three workshops and additional resources.
- Our team will also engage in **research activities**, while disseminating our results and creating **partnerships**.

### FRISCO INSIGHTS

After [discussions with more than 50 HSPs](#) and other relevant stakeholders, we have found that:

- Small platforms are **heavily targeted** by terrorists but some more than others due to the types of services they offer, namely file storage, file sharing, archiving, and content pasting.
- Small platforms currently have a **very limited awareness and knowledge** of the TCO Regulation but perceive themselves to be at low risk of being exposed to terrorist content.
- Most of the small-scale HSPs are currently **missing the core infrastructure and the appropriate resources** to identify, monitor and remove terrorist content, and comply with the TCO Regulation.

### FRISCO WHAT WE HAVE TO OFFER

To [respond to these gaps](#), the FRISCO Project has a lot to offer to HSPs:

- **Multi-stakeholder collaboration:** we encourage collaboration between HSPs and other stakeholders (e.g. LEAs) to better combat the threat together.
- **Knowledge of the legal framework:** we offer practical advice and resources to help HSPs better understand the legal framework and the specific steps they need to take to comply with it.
- **Free and actionable resources:** we develop free resources for HSPs to foster their compliance with the TCO Regulation and counter the terrorist exploitation of the Internet.

- **Practical examples:** we highlight case studies and real-life examples of practices employed by stakeholders to moderate and deal with terrorist content online.

- **Workshops and consultations:** we engage with LEAs, HSPs, industry associations, researchers and experts to gather insight, learn from each other and create a safer online environment.

The FRISCO project aims at sharing experiences and best practices amongst the targets and other stakeholders part of the project.

Based on the insights gathered from our Multi-stakeholder event and the Best Practices Manual, this brochure is designed to equip HSPs with a comprehensive list of technical solutions. These tools are aimed at facilitating full compliance with the TCO regulation.

The solutions are offered by a diverse range of service providers, each specialising in various software-based anti-terrorism measures. These span from specific detection tools to all-inclusive content moderation software and advanced hash-matching tools.

These providers form an integral part of our global ecosystem, collectively striving to make the internet a safer place for all by preventing the dissemination of harmful and illegal content.

This brochure, therefore, serves as a platform for fostering collaboration among various stakeholders. It encourages the creation of synergies and promotes the sharing of experiences, ultimately contributing to a safer digital environment for everyone.

### **3 Approach for Work Package and Relation to other Work Packages and Deliverables**

The project is delivered through five Work Packages (WPs). WP1 will manage and coordinate day-to-day management activities of the project. WP2 is dedicated to the development of relevant tools. WP3 aims to create a training program and to develop e-training modules, while WP4 helps raise awareness of HSPs. WP5 is dedicated to the dissemination and exploitation of results.

This deliverable is connected with the WP2 by sharing the three tools - the self-assessment questionnaire, the process map, and the content moderation software - developed within the FRISCO project as a first basis for HSPs to use. Additionally, this document goes further by offering other tools specialised in parallel services provision and sharing expertise that the FRISCO project could not touch on due to its limited scope. We hope that this document will prove valuable to HSPs, enabling them to find tailored tools that cater to their unique needs within the industry. By doing so, we aim to support HSPs in enhancing their services and contributing to a safer online environment.

#### **3.1 Methodology and Structure of the Deliverable**

The companies listed in this document have been contacted to participate in our marketplace session on the 18-19th of April 2024, where they had the possibility to pitch their solutions and services to the HSPs invited. They were requested to answer the following questions:



1. Please indicate the country of your company
2. Please provide the website url of your company
3. Company Overview: Please provide a brief description of your company's background and mission
4. Services Offered: Please provide a description of the service(s) provided by your company
5. Targets: Please indicate the main targets/audience of your services
6. Please indicate how you can support HSPs
7. Pricing and Licensing: Information on the cost structure and licensing options for the solution, including any available discounts or packages for HSPs
8. Logo: Please share with us your logo (.png format):

The answers to these questions were used as the basis for the content of this document. Additional information was retrieved by contacting the companies independently and through the information available on their website.

This document provides a description of the services and solutions provided by these companies within the context of the TCO regulation. Each company will have a section of its own with its information. This document will then be put into a different document to enhance user-friendliness through graphic design.

The tools were put in four different categories

1. **FRISCO tools**
2. **Content moderation software:** These tools offer a full content moderation software including detection tools
3. **Detection tools:** Tools that offer analysis systems for detecting harmful or illegal content using AI systems.
4. **Hash matching tools:** Hash matching tools are software solutions that use cryptographic hash functions to compare digital files or data sets and identify matches or similarities between them.

## 4 FRISCO tools

### Self-assessment questionnaire

The self-assessment questionnaire aims at helping small and medium HSPs understand their level of compliance with the TCO. This questionnaire is meant as a first step for HSPs to understand how their current internal processes for content moderation regarding terrorist content align with the TCO Regulation. The objective of this tool is to provide HSP with a compliance score, which helps them situate themselves in the path to full TCO compliance.

Available [here](#)

### Process map

FRISCO's process map is an interactive tool that structures and describes the entire compliance process with the TCO Regulation and related duties for HSPs in a holistic way, so to say from the exposure to terrorist content to the transparency reports. This tool, focused on HSPs' operational needs, provides a precise breakdown of the TCO Regulation, step by step, and is based on a holistic and chronological approach to compliance. The process is displayed gradually, thanks to interactive and/or animated transitions, and the whole map can be downloaded entirely in the end. Legend, colour code and steps increase ergonomics and user's experience. Finally, more information, resources and tools are made available via the tool.

Available [here](#)

## 5 Content moderation software

### FRISCO Content moderation tool - Tremau - France

<https://friscoproject.eu/content-moderation-tool>

FRISCO's content moderation tool is a user-friendly trust and safety tool that addresses user-generated content related risks. The tool is based on Tremau's in-house solutions and tailored to hosting service providers' needs in relation to the new regulations such as the TCO, thanks to the project's findings and resources. As a small HSP, you face unique challenges in ensuring that your platform remains free from any form of harmful content, including terrorist-related materials. Our purpose-built Content Moderation Tool is here to assist you in this critical mission by moderating all content, no matter the source of detection, in one place; streamlining their moderation process; generating operational efficiencies (of up to 50%); achieving better control and transparency; ensuring consistent application of their Terms of Service and Community Guidelines and customising queue management and prioritisation rules.

Key features include:

- All data signals in one place
- AI powered end-to-end moderation platform integrating all detection sources
- Manual and automated processing
- Compliant by design
- Built to power content moderation best practices

If you're interested in a demo or have any questions, please feel free to reach out to us at [info@friscoproject.eu](mailto:info@friscoproject.eu) or [info@tremau.com](mailto:info@tremau.com) directly. Our team is ready to provide you with more information and guide you through the capabilities of the Content Moderation Tool.

### Utopia Analytics - Finland

<https://utopiaanalytics.com>

Utopia Analytics is a Finland based company serving different industries since 2014, that enables automated moderation with its proprietary AI to identify inappropriate content or behaviour, hate speech, discrimination, sexual harassment, spam, etc. Online content is automatically filtered out 24/7 to allow teams to focus on moderation policy management. Utopia AI Moderator is a fully automated moderation tool that protects your online community and your brand from abusive user-generated content, fraud, hate-speech and illegal content. The AI learns from previous publishing decisions made by your team, works in real-time, with a higher degree of accuracy than traditional tools and it is ready for production in only 2 weeks.

Key features include:

- **Rule making:** The user can develop its moderation policies. The system subsequently learns from moderator decision-making to apply these rules.
- **Functional features:** Utopia AI moderator can define the reasons why a particular content was flagged
- **Social media language:** Utopia AI moderator understands the semantic meaning of social media language regardless of spelling errors, informal grammar use or unusual meanings of words.
- **Image and video moderation:** Utopia AI analytics also provides automated video and image moderation.

Utopia Analytics works with leading organisations in their fields, collaborating across several different industries such as: online platforms, news media companies, social media platforms, online marketplaces, gaming and dating companies, reviews sites, among others. This tool can help overcome the challenges related to user-generated content moderation while implementing solutions that help you comply with legislations and regulations such as Digital Services Act (DSA).

**Pricing information:** Utopia Analytics services are offered as Software as a Service (SaaS) with very competitive prices based on the requirements of the project. For more information contact [utopiaanalytics.com](https://utopiaanalytics.com)

### Bodyguard - France

<https://bodyguard.ai>

Bodyguard.ai helps businesses from all industries in **curating their user-generated content in multiple languages and across multiple platforms and social media in real-time**. Bodyguard's content moderation software has an advanced AI and NLP technology, provides the best contextual analysis of the market, allowing clients to better understand their audience and make informed decisions to improve their social media strategy.

Key features include:

- Dedicated dashboard with valuable insights and actionable data
- Context-aware analysis of user-generated content
- Sentiment analysis
- Special Sport and Gaming applicability.

By filtering out irrelevant content and identifying valuable user-generated content organisations can help promote their brand and engage with their customers safely. Thanks to real-time analysis, this tool can respond quickly to potential crises and ensure that their online presence remains positive and engaging.

**Pricing information:** Please contact Bodyguard using their contact [form](#).

## 6 Detection tools

### Sightengine - France

<https://sightengine.com>

Sightengine offers Automated Content Moderation models and tools to analyse images and videos based on Natural Language Analysis and Proprietary Algorithms. These tools come via API integration and offer 60+ moderation categories across nudity, hate, violence, drugs, weapons, self-harm and more that are context-aware. These tools are highly customizable and can be tailored to clients needs: It is available in many languages to support users from any region and can be used on messages, chats, user profiles, usernames, comments or reviews in real-time. Whenever there is a match, the Sightengine API gives a tag describing the type of content found along with its position in the text, so the user can easily remove the offending phrase, change it or block the entire message.

Key features include:

- Choice of the filters to apply
- Prevention of users bypassing these filters by detecting millions of variations for each unwanted word: letter replacements, character insertions, phonetic variations, leet speak, obfuscation, hyphenation, special characters, embeddings etc.
- Offers the possibility to decide when users should be allowed to share links and web URLs by implementing a whitelist/blacklist of specific URLs and domains.

Sightengine has been working with social media platforms, service providers, marketplaces and apps for more than 10 years.

**Pricing information:** Sightengine offers different pricing plans depending on the specific needs with a free version available. See the full information [here](#).

### Textgain - Belgium

<https://textgain.com>

Textgain was founded in 2015 as a spin-off of the University of Antwerp (Belgium) and offers a full range of customizable data management and analysis solutions to sort incoming emails, extract insights from PDFs, follow the news, or discover opinions on social media. They specialise in the development of Artificial Intelligence that automatically detects and monitors harmful societal trends and tensions, such as hate speech and disinformation.

Textgain offers different tools:

- **Text Analytics API:** Textgain's Analytics API offers a collection of diverse NLP tools to help infer insights from text data: age detection, sentiment analysis, gender prediction,

language-specific grammar and lexical analytic features, polarity calculation, etc. Built on R&D at the University of Antwerp, this product is multilingual (available in 15 languages), without server-side data retention.

- **SentiMeter:** SentiMeter is a data analytics dashboard that uses the official Textgain API to measure online sentiment among citizens of a specific geographical area, like a city, municipality or province. It is customizable for social media platforms or websites to be monitored, topics, locations, etc. Sentimeter isolates social media data for this area based on geolocation, trigger words and local public accounts. Various NLP strategies are applied on the collected data to perform sentiment analysis and detect trends and shifts on social media. As SentiMeter collects more data, it will be able to provide an increasingly accurate representation of the sentiment, questions, and other issues shared among citizens.
- **Grasp:** Grasp is a free, lightweight AI toolkit for Python, with tools for data mining, NLP, machine learning and network analysis. Grasp is a multifunctional toolkit with tools for data mining, including downloading and processing html, finding ready-to-process wikipedia articles and twitter opinions, as well as easily deploying API's. The natural language processing toolkit includes tools for language identification, finding words, sentences, and word types, as well as determining the polarity of a text. Grasp's network analysis toolkit includes seamless functions to map and visualise networks. The machine learning toolkit includes algorithms to quantify text, train models, and retrieve predictions. Machine Learning algorithms learn by example. By showing them 10K spam and 10K real emails (i.e., train a model), they can predict whether other emails are also spam or not.
- **Panorama:** Panorama is an award-winning explainable AI framework for real-time, multilingual social media analysis. It includes a dedicated annotation app, GDPR-compliant anonymization algorithms, anonymous user profiling (age, gender, etc.), named entity recognition, and a stunning visualisation toolkit (charts, graphs, trees, etc.). It detects toxic content in all EU languages (and Arabic, Turkish, Russian) on dozens of online platforms, with fine-grained labelling of ridiculing, dehumanising, discriminatory, misinformative, violent and/or extremist content, carefully curated by 50+ local language experts. Most of all, it is a very lightweight program that does not require heavy hardware. The Panorama package also contains a visualisation component to help the user make sense of their data.

In 2021, Textgain became the coordinator of the European Observatory of Online Hate, an initiative to monitor online hate speech across the European Union.

**Pricing information:** Pricing will depend on the tool. For more information please contact [info@textgain.com](mailto:info@textgain.com).

## Identrics - Bulgaria

<https://identrics.ai>

Identric is an award-winning research and development company that creates AI-based solutions for publishing, media and risk intelligence - from ready-to-use models, to fully tailored data science services. These AI-based solutions help organisations of all sizes and the people in them, deal with immense volumes of data and text. Our algorithms delegate organisations' menial data and text processing tasks to machines, so that humans can focus on high-end, insight-oriented work. Solutions range from data classification and indexing, to content enrichment – such as named entity recognition, sentiment analysis, all the way to automated content recommendation and generation.

Services include:

1. **Natural Language Processing Enrichments:** A service that enhances text data with contextual information, enabling better understanding and analysis of unstructured data.
2. **Topic Engagement:** A tool that analyses user interactions with specific topics, providing insights into audience engagement and interest levels.
3. **Hate Speech Detection:** A service that automatically identifies and flags hate speech in user-generated content, helping to maintain a safe and respectful online environment.
4. **Propaganda and Disinformation Detection:** A tool that detects and categorises misleading or false information, assisting in the prevention of its spread and mitigating its impact.
5. **Abstractive Text Summarisation:** A service that generates concise summaries of lengthy texts, providing a quick overview of key information without losing the original context.
6. **Automated Reports and Newsletters:** A tool that streamlines the creation and distribution of reports and newsletters, saving time and resources while ensuring consistent and accurate communication.
7. **Media Contacts Database Automation:** A service that automates the process of building and maintaining a database of media contacts, enabling efficient and targeted outreach.
8. **Custom & DSaaS:** Customised data science solutions and Data Science as a Service (DSaaS) offerings that cater to specific business needs, providing tailored insights and analytics.

Identric's disinformation detection services cater to the needs of a diverse audience, including: Research centers, Law enforcement agencies, Educational institutions, Government bodies, Media organisations, Fact-checking organisations, and online hosting service providers.

**Pricing information:** For information about the pricing, please use the contact form [here](#).

### Logically AI inc. - UK

<https://logically.ai>

Logically is a tech company identifying malign influence operations and harmful content on the internet. Logically has produced a U.S. Domestic Extremism Content Classifier. Founded in 2017, now working with governments and organisations around the world. Logically's Domestic Extremism Content Classifier is an AI model that can identify pieces of online, text-based content within our software solution called, Logically Intelligence, that represent indicators of U.S. domestic extremism. The model specifically focuses on identifying content that could represent hate speech,

indoctrination, radicalization, recruitment, or plotting related to anti-LGBTQIA+, racially/ethnically motivated, or antigovernment authority violent extremism. While our classifier is up and running on U.S. domestic extremism, the process and methodology we used is repeatable across cultures and languages.

Key features:

- Counter Narrative Strategies
- Event Influence Assessment
- Group Actor Analysis
- Influence Campaign Attribution
- Misinformation and Disinformation Analysis
- Policy and Strategy Formulation
- Trend Analysis for Fact-Checking
- Adaptable to different languages

**Pricing information:** There are three offering; purchase of the domestic extremism classifier, the purchase of Logically intelligence that includes the U.S. domestic extremism classifier and other threat classifiers; or technical services work to design and build an extremism classifier tailored to a different language and culture. For access to the Logically Intelligence platform's U.S. domestic terrorism product is approximately \$5,000 per month. To develop terrorism threat classifier to match a regions terrorism problem requires a discussion with the DevOps team in order to provide a quote.

## ALLIES project

<https://alliesproject.com>

The ALLIES project is part of the TCO cluster and aims to support micro and small HSP in achieving compliance with the new requirements and obligations under the “Terrorist Content Online” (TCO) Regulation. This is achieved through the creation of proper learning, training, experience sharing mechanisms as well as technical AI tools. Their AI tools are specifically designed and tailored for HSPs.

Key feature include

- Text analysis
- Multilingual speech recognition
- Video and Image recognition
- Multimodal data hashing
- Risk assessment for content

**Pricing information:** The tools are free to use.



## 7 Hash-matching tools

Hash-matching is a fingerprinting technology that allows the creation of a hash for a piece of content (i.e. image, text audio, video) and then compares it to existing database of prohibited hashes allowing to flag illegal content.

### Web-IQ - Netherlands

<https://web-iq.com>

Web-IQ is an IT company based in the Netherlands, using Open-Source Intelligence (OSINT) to help organizations fight serious crimes, like fraud, child abuse and human trafficking.

Their Hash Check Service transforms any image or video into a hash, which is the digital fingerprint of a file in the form of a code, to its central database of known child sexual abuse material. The user receives an answer as to whether this hash occurs on lists of hashes provided by e.g. the Dutch National Police. This service is provided through an HTTP based API. The Hash Check Service is a service offered by the Dutch hotline Offlimits and Web-IQ.

The Hash Check Service is meant for Internet Service Providers (ISP's), hosters and Trust & Safety organisations. The purpose behind the Hash Check Service is to increase the speed with which online child sexual abuse material can be detected and removed from the internet. With the Hash Check Service HSPs can tap into many databases of known child sexual abuse material with an easy integration. In those efforts, Web-IQ has been collaborating with Tax Authorities, Financial Services and Law Enforcement agencies for over 10 years.

**Pricing information:** Any ISP or hoster from a country that is part of the INHOPE organisation can use the Hash Check Service for free.

### Tech Against Terrorism

<https://techagainstterrorism.org/home>

Tech Against Terrorism is an independent, public-private partnership launched by the United Nations in 2016. They work with the tech sector and are supported by the UN as well as by other international bodies including the governments of the United Kingdom, Spain, Switzerland, the Netherlands, the Republic of Korea, and Canada. Their work revolves around threat intelligence, technical innovation, and policy advice. Tech Against Terrorism offers a Terrorist Content Analytics Platform (TCAP), a content moderation tool for tech platforms, enabling the detection and removal of terrorist content through open-source intelligence and connected to a Hash-Matching database.

Key features

- Content reporting and moderation
- Automated content alert

- Automated status checks to determine if collected content is still online as well as automated archiving and hashing of content.

Additionally, Tech Against Terrorism offers TCO training material and a knowledge sharing platform and strives to empower and educate tech platforms to improve their existing counterterrorism responses.

**Pricing information:** [contact@techagainstterrorism.org](mailto:contact@techagainstterrorism.org)

## 8 Final insights

As part of the FRISCO project, this document was created to provide HSPs access to a variety of solutions that can help them with TCO compliance and fight back against terrorist content online.

The brochure overviews a total of 12 tools from various service providers. These tools are divided into 4 categories: (1) FRISCO tools, (2) content moderation softwares, (3) Detection tools, (4) Hash-matching tools. Through these 4 categories, we hope to cover enough grounds to allow HSPs to find tools tailored to their specific needs and facilitate TCO compliance as well contribute to emerging collaboration in online anti-terrorist activities.

-----End of Document-----