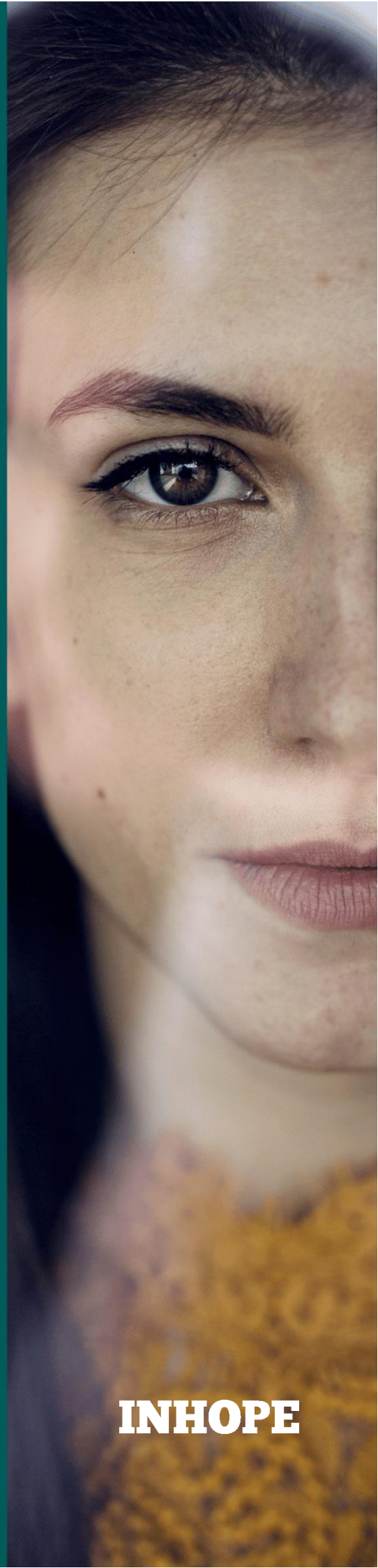


Fight CSAM.

Learn more and get involved: [*Inhope.org*](https://inhope.org)

Trusted Flagger Program

INHOPE



Background

INHOPE hotlines and other recognised organisations (e.g. Helplines) are known as good actors which facilitate the public to report illegal content that they may find on the internet. As they have built relationships with online service providers and platform operators over the years – their reports are often treated as pre-qualified and in many cases are prioritised for action. This process originally evolved from an informal system started in 2018 and evolved to the point that today the trusted flagger program is a standardised process ensuring that reports from recognised Trusted Flagger Hotlines are expedited leading to the rapid removal of the content.

To join the INHOPE Trusted Flagger program – INHOPE must be satisfied that the organisation is committed to the program and the rapid removal of illegal content on their platform. If this is confirmed, then a reporting exchange procedure is agreed with the platform and this is shared with INHOPE member Hotlines. Following this – any reports received from relevant INHOPE member Hotlines will be prioritised and treated as pre-qualified.

Digital Services Act (DSA)

The DSA created a formal legal basis for Trusted Flagger recognition within the European Union and places a legal requirement on companies to act on reports received from recognised organisations like hotlines. It states – (Recital 46) *“Such entities can be public in nature, such as, for terrorist content, internet referral units of national law enforcement authorities or of the European Union Agency for Law Enforcement Cooperation (‘Europol’) or they can be non-governmental organisations, consumer organisations and semi-public bodies, **such as the organisations part of the INHOPE network of hotlines** for reporting child sexual abuse material.”* The regulation specifically states – ‘Notices submitted by trusted flaggers must be processed and decided upon with priority and expeditiously’.

INHOPE Trusted flagger technical implementation

This is quite straight forward and just requiring some basic elements. Main challenge is to agree the process for when the system is up and running. Below is a potential scenario:

1. Partner creates an email address (e.g. TrustedFlaggerReport@partner.com) which will result in emails to this address being rapidly reviewed by abuse team.
2. INHOPE & Partner create a one-pager info sheet for hotlines, and this is shared with all Hotlines – where hotlines can opt-in to the trusted flagger via an online form managed by INHOPE.
3. After a specified deadline all of the Hotline responses will be checked, and identity validated by INHOPE.
4. The validated list of email addresses of ‘Partner trusted INHOPE flaggers’ will be shared with Partner by INHOPE.
5. Any reports received by Partner via TrustedFlaggerReport@partner.com from any of the email addresses from the previous point should be escalated as a priority.
6. Any later registrations of Hotlines after the deadline will be shared by INHOPE ASAP to update the trusted list.

Interested? Contact our Head of Partnerships & Network Expansion, Samantha Woolfe: samantha.woolfe@inhope.org