Code of Conduct for Notice-and-Take-Down

BIT B.V.

Version 2.0: July 2026

The Digital Services Act (DSA) places due diligence obligations on providers of intermediary services, such as cloud and hosting companies, in handling notices of illegal content online. What the DSA refers to as "illegal content" is referred to in this code of conduct as unlawful or criminal content.

Society must be able to trust that providers of intermediary services make efforts to remove unlawful and criminal content from the internet.

This Code of Conduct for Notice-and-Take-Down (hereinafter referred to as "code of conduct") is aligned with the DSA, Dutch legislation, and practical experience within the sector. It replaces earlier sector-specific arrangements and is intended to provide providers with practical guidance in applying their obligations.

Scope of notices and procedures

This code of conduct applies to voluntary **notices**: requests made by notifiers to providers of intermediary services to have unlawful or criminal content removed from the internet.

Outside the scope of this code of conduct fall orders from competent authorities, such as the **ATKM, law enforcement agencies**, or the **Public Prosecutor**. For such orders, legal frameworks and procedures apply; providers are required to comply with these regardless of this code of conduct.

For notices that do fall within the scope of this code of conduct, the procedures as described in this code of conduct apply. In addition, supplementary arrangements have been made for certain categories of content, such as with **Offlimits** for notices regarding child sexual abuse material. These arrangements are set out in a separate addendum.

Definitions

- **Provider of intermediary services**: a provider of digital infrastructure that facilitates public access to internet services in the Netherlands, including mere conduit, caching, and hosting services, and therefore not for the VLOPs (Very Large Online Platforms) as described in the DSA.
- **ATKM**: the Authority for Online Terrorist and Child Sexual Abuse Material, authorized to issue removal orders for terrorist content and child pornography (CSAM).
- **Competent authority**: an entity with statutory authority to demand information or removal, such as the ATKM or a law enforcement agency.
- **Content provider**: the person or entity that has placed certain (contested) content on the internet.
- **Notice**: the act of a notifier reporting (alleged) unlawful or criminal content on the internet to a provider of an intermediary service, with the aim of having that content removed.
- **Notifier**: the person or entity that submits a notice.
- **Offlimits**: the foundation that in the Netherlands receives, assesses, and issues NTD requests for child sexual abuse material and, where necessary, forwards these to competent authorities.
- **Manifest illegality**: content that is demonstrably in violation of the law or the rights of third parties without the need for in-depth investigation.
- **Law enforcement agency**: a legally designated entity with authority for supervision or investigation, such as the police or the Public Prosecution Service.
- **Trusted Flagger**: a notifier recognized as a reliable party whose notices are handled with priority. This includes both trusted flaggers designated by the European Commission under Article 22 of the DSA, and parties designated as such by a provider of intermediary services.

Handling of notices

Providers of intermediary services maintain a publicly accessible procedure for handling notices of unlawful or criminal content.

A notice contains at least the elements as set out in Article 16, paragraph 2 of the Digital Services Act:

- the name and contact details of the notifier;
- the location of the content (for example, a URL or IP address);
- a description of why the content is considered unlawful or criminal;
- a declaration that the notice is, to the best of the notifier's knowledge, accurate and complete

Notifiers are preferably requested, where possible, to first approach the content provider before directing the notice to another party. When submitting a notice, they should briefly explain why it is directed at the relevant party and what steps have already been taken to have the content removed through earlier links in the chain (such as the content provider).

Step-by-step approach for notices

When addressing notices, a step-by-step approach is applied. The starting point is that the content provider is approached first, followed by the provider of an intermediary service (such as a hosting provider), followed by other intermediaries such as registrars or access providers, and finally the registry. This approach is consistent with the principle of proportionality and minimizes the risk of unintended or disproportionate removal of content.

Assessment and measures to be taken

The provider confirms receipt of a notice within one working day and informs the notifier whether the notice will be processed. For urgent notices or notices from Trusted Flaggers, a faster response is provided.

Following receipt of a notice, the provider of an intermediary service assesses whether the content constitutes manifestly unlawful or criminal content. The assessment is completed within one working

day of receipt of the notice. If the assessment requires more time, the notifier is informed with a justification; the assessment is in that case completed no later than within five working days.

If the provider concludes that the content constitutes manifestly unlawful or criminal content, the provider ensures that the relevant content is removed or made inaccessible promptly, but in any case, within one working day of receipt of the notice.

If no clear conclusion can be reached, the content provider is notified of the notice with a request to voluntarily remove the content or to contact the notifier. If the provider concludes that the content does not constitute unlawful or criminal content, the provider notifies the notifier accordingly with a justification.

Communication

When content is removed or restricted, the provider informs the relevant content provider of the measure taken and the reason for it, unless legal provisions prohibit this. The identity of the notifier is not shared if the notifier has indicated wishing to remain anonymous.

The provider informs the notifier of the outcome of the assessment. If no measure is taken, the provider provides a justification.

Zorgvuldigheid en proportionaliteit

Providers take measures that have as little impact as possible on other users or services. Only the content to which the notice relates is removed or made inaccessible. Removal of more information than strictly necessary is avoided.

Hosting providers that become aware of information giving rise to a suspicion of a criminal offence in which the life or safety of one or more persons is threatened, shall immediately report this to the competent authorities and provide all available relevant information. This follows from Article 18 of the Digital Services Act.

Revision and management

This Code of Conduct for Notice-and-Take-Down will be reviewed annually, based on regulations, feedback and experiences of the participants in this code of conduct. With each revision, the version number will be updated, and changes will be documented in the revision history. NBIP is the owner of this code of conduct and responsible for version control.

Code of Conduct Representatives

The following organizations have actively contributed to establishing this Code of Conduct:

- Stichting Digitale Infrastructuur Nederland (DINL)
- Dutch Cloud Community (DCC)
- Nationale Beheersorganisatie Internet Providers (NBIP)
- Vereniging van Registrars (VvR)

Code of Conduct Endorsers

The following organizations endorse the principles and objectives of this Code of Conduct and commit to promoting and adhering to these standards:

- Anti Abuse Netwerk (AAN)
- Belastingdienst
- Dutch Data Center Association (DDA)
- ECP | Platform voor de InformatieSamenleving
- Internet Society Nederland
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Ministerie van Economische Zaken en Klimaat

- NL Digital
- Offlimits
- Openbaar Ministerie
- SIDN
- Stichting BREIN

Revision History

Version 2.0 – July 2026

- Comprehensive revision based on practical experience, technological developments and new legislation, including the Digital Services Act.
- Clarification of the scope: distinction between notices (voluntary, within the scope of this code) and orders from competent authorities (outside the scope of this code).
- Timelines clarified: acknowledgement of receipt, assessment, and removal within one working day.
- Clarification of the anonymity clause: the identity of the notifier is not shared without consent.
- Adjustment of the Trusted Flagger provision in accordance with Article 22 of the DSA.
- Annual review and version management under the responsibility of NBIP.

Version 1.1 – December 2018

- Addition of addendum on notices via EOKM (now: Offlimits).
- Establishment of 24-hour removal obligation for notices of child pornography.
- Exclusion of liability of EOKM for incorrect notices.

Version 1.0 – October 2008

- First version of the sectoral Code of Conduct for Notice-and-Take-Down, drawn up by ECP in cooperation with providers and government.
- Introduction of principles such as manifest illegality, step-by-step approach and proportional content removal.
- Voluntary guideline for providers of intermediary services.

Addendum 1: child sexual abuse material, Offlimits as notifier

1 Subject and scope

This is an addendum to the Code of Conduct for Notice-and-Take-Down (hereinafter: the Code of Conduct). It sets out specific arrangements that deviate from and supplement the Code of Conduct. Where the text of the Code of Conduct and this addendum conflict, the text of this addendum prevails.

This addendum concerns the notice and take-down of manifestly criminal images of minors (child pornography), as defined in Article 252 of the Dutch Criminal Code and further developed in applicable case law.

2 Offlimits as Trusted Flagger for VLOPs

Offlimits has been designated by the ACM as a Trusted Flagger for VLOPs (Very Large Online Platforms) under the Digital Services Act (DSA), on the basis that Offlimits holds the specific expertise and authority to identify and report illegal content. That expertise covers, among other things, child sexual abuse material (Article 252 of the Dutch Criminal Code).

Where an online platform is required to comply with Article 22 of the DSA, a removal request is submitted through a reporting mechanism as referred to in Article 16 of the DSA. That request is sent from the email address hotline@trustedflagger.offlimits.nl. The online platform is expected to handle the removal request with priority and within a reasonable time.

3 Offlimits as notifier to hosting parties that are not required to comply with Article 22 of the DSA

a. The investigation and prosecution of child sexual abuse material is reserved to the competent law enforcement authorities, and orders issued in the context of criminal prosecution are separate from notices submitted under this Code of Conduct.

b. For all notices concerning child sexual abuse material, an approach has been agreed with the competent law enforcement authorities. These arrangements are set out in a protocol between Offlimits and the Public Prosecution Service. In situations where immediate action can be taken to render material inaccessible, Offlimits contacts the intermediaries concerned.

c. Accessing and viewing (potential) child sexual abuse material is a criminal offence and may lead to prosecution. In order to carry out its work, Offlimits has been granted an exemption from prosecution by the Public Prosecution Service for specified acts and under predetermined conditions.

d. Offlimits is a member of INHOPE, the global network of hotlines dedicated to combating online child sexual abuse.

e. Offlimits is an expert in assessing child sexual abuse material and has demonstrated over the years that it submits reliable notices in this field with due care. Under this addendum, Offlimits only submits a notice where it has carefully established beyond doubt that the material constitutes child sexual abuse material. These notices are sent from the email address info@meldpunt.offlimits.nl.

f. Offlimits holds a unique position in the Netherlands, and the participants in this addendum therefore regard Offlimits as an important and demonstrably reliable notifier of child sexual abuse material in the Netherlands.

g. Intermediaries process notices from Offlimits concerning child sexual abuse material without assessing for themselves whether the content is manifestly unlawful or criminal.

h. Intermediaries do not invoke the option of requesting an explicit indemnity from Offlimits against claims by the content provider resulting from measures taken in response to the notice.

4 Removal within 24 hours

Intermediaries ensure that the content to which a notice from Offlimits relates is removed or made inaccessible promptly, and in any case within 24 hours of receipt of the notice.

5 Description of the Offlimits reporting process

a. Offlimits receives notices through various channels. Members of the public can submit a report through the form on its website. Reports from other hotlines worldwide are received through the international INHOPE network. Offlimits also receives reports from the police.

Offlimits works from an overview of open reports. Where a report is found to contain criminal material, it is established where that material is hosted. If the hosting is located outside the Netherlands, it is checked whether that country is connected to the INHOPE network. If so, the report is forwarded to the hotline of that country.

Where the hosting provider is established in the Netherlands, Offlimits verifies the hosting details through various sources. The information required includes the hosting provider, the IP address, the country of hosting and the abuse email address.

For illegal material hosted in the Netherlands, the system automatically sends a Notice and Take Down request (NTD) to the relevant abuse email address. The structure of that NTD request is included as a model message at the end of this addendum.

b. The Offlimits reporting process deviates from the process described in the Code of Conduct for Notice-and-Take-Down.

Offlimits approaches the provider of intermediary services (the hosting party) first, before directing the notice to any other party. If no action follows within the stated time limits, Offlimits may turn to another party, such as another intermediary (for example a registrar or access provider) or the content provider (for example the owner of the website).

In particular cases, Offlimits deviates from this process. For instance, arrangements exist with certain websites whereby an NTD sent to the provider of intermediary services is accompanied by an NTD to the content provider at the same time, in order to speed up the removal of illegal content.

Model NTD request

Subject: Report on Child Sexual Abuse Material

Dear Sir/Madam,

Who we are

The Dutch Hotline (Meldpunt Offlimits) is an independent private foundation which fights against online child sexual abuse material (CSAM). Also, the Dutch Hotline is one of the founders of INHOPE, the global network of hotlines against online CSAM. The procedure to report online CSAM, together with supporting information, is published on our website. The Dutch Hotline receives subsidies from the Dutch Ministry of Justice and Security and the European Commission. Since its founding the Dutch Hotline has closely cooperated with the Dutch police and since July 2024 with the Authority for the prevention of online Terrorist Content and Child Sexual Abuse Material ATKM.

The Dutch Hotline would like to make you aware that the reported URL below contains CSAM as assessed under Dutch law. Therefore, we are sending you this notice and takedown, and request you to take action and to remove the content/URL. If the reported URL is not removed/made inaccessible within 24 hours, the Dutch Hotline (Meldpunt Offlimits) will inform the ATKM. Subsequently, the ATKM can order the removal or inaccessibility of the URL and enforce compliance by imposing penalties according to Dutch legislation. More information regarding the ATKM and the legislation, see: www.atkm.nl.

Invitation to use the free online Hash Check Service

The Dutch Hotline has developed an online tool to help hosting providers and website owners to prevent the dissemination of CSAM on their services. The tool enables parties to check MD5 and SHA-1 hashes of images with the hash-database consisting of known CSAM. This will help hosting providers and website owners to prevent users from uploading CSAM on their services. The tool is provided to interested parties free of charge and on a voluntary basis. A technical description of the Hash Check Service can be found here. We would like to invite your organization to be part of this program. To do so, please reply to this email.

Reporting Child Sexual Abuse Material

```
BEGIN
URL:
   url           IP            First seen    Last seen     Note
   ------------- ------------- ------------- ------------- -------------
   VOORBEELD A   VOORBEELD A   VOORBEELD A   VOORBEELD A   VOORBEELD A
   VOORBEELD B   VOORBEELD B   VOORBEELD B   VOORBEELD B   VOORBEELD B
END
```

Should you require any further information regarding this matter, please contact us by email info@meldpunt.offlimits.nl.

Kind regards,

Meldpunt Kinderporno op Internet | Dutch hotline against child sexual abuse material on the Internet
https://meldpunt.offlimits.nl/

DISCLAIMER:

No rights may be derived from this message and/or this attachment (these attachments). Important agreements must therefore always be signed by an appropriately authorized individual. This mail is intended for the addressee's (addressees') eyes only. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this information is strictly prohibited and may be unlawful. If you have received this communication in error, please notify us immediately by responding to this email and

then delete it from your system. It may not be distributed to, nor used by, third parties. https://offlimits.nl/ Offlimits disclaims any liability arising from electronic mailing.