DIGITAL

Transparency Report

as per Article 8 of the Terrorist Content Online Regulation and section 4 of the Act addressing terrorist content online and Monitoring Report as per Article 21(1) of the Regulation and section 3 of the Act

Bundesnetzagentur

Transparency Report as per Article 8 of the Terrorist Content Online Regulation and section 4 of the Act addressing terrorist content online and Monitoring Report as per Article 21(1) of the Regulation and section 3 of the Act

Year under review: 2025

As of March 2026

Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen

Section 905 Addressing Terrorist Content Online, Data Regulation

Tulpenfeld 4
53113 Bonn
Germany
Tel. +49 (0)228 14-0
Fax +49 (0)228 14-8872
Email info@bnetza.de

Contents

Contents **3**

1. Foreword 4
2. Transparency report/Monitoring report 6
3. Summary/outlook 10

Publisher's details **11**

1. Foreword

Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online ("Terrorist Content Online Regulation") entered into force on 7 June 2021. The Regulation aims to address the misuse of hosting services for terrorist purposes and thus contribute to public safety in the European Union. The Regulation is intended to prevent the internet from being used by terrorists to spread their message in order to intimidate and radicalise people, to recruit followers and to enable terrorist attacks. This is particularly relevant in times marked by conflict and instability.

Hosting service providers are providers who offer the storage and dissemination of information on the internet by technical means, and who store and disseminate content to the public on behalf of a content provider. They connect companies and people, enable public debates and the dissemination and receipt of information, opinions and ideas. Thus they play a key role on the internet. However, third parties sometimes use hosting service providers to conduct illegal activities on the internet. Particularly worrying is the misuse of these services by terrorist groups and their supporters with the aim of disseminating terrorist content online and thus spreading their message, radicalising and recruiting followers, as well as enabling and directing terrorist activities.

For several years, voluntary cooperation efforts have been made at the European Union level between the Member States and the hosting service providers to address online terrorist content. The Regulation gives these efforts a clear regulatory framework that aims to address the misuse of hosting services for terrorist purposes and further mitigating access to online terrorist content.

The Regulation imposes obligations on hosting service providers and gives the competent authorities additional tools. The main tool is a removal order, which can be issued by a competent authority to a hosting service provider. Hosting service providers must remove terrorist content within one hour of receiving a removal order. The content must be removed promptly because terrorist content is disseminated very rapidly through online services. Before the Regulation came into effect, the only available tool was a removal request, which is still used in part by European authorities as a preliminary step before issuing a removal order.

Hosting service providers are subject to further obligations if their service is used repeatedly to disseminate terrorist content. In this case, hosting service providers must take "specific measures" (content moderation) to better protect their hosting service in the future from misuse by terrorists disseminating terrorist content online. Hosting service providers are free in their choice of which measures to adopt and may therefore make use of both technical and organisational tools. It is important that the measures to be taken or that have been taken are effective in order to counteract the dissemination of terrorist content online. The measures employed may include proactive moderation (eg automated filter systems or content hashing algorithms) or reactive moderation (eg manual moderation or community supported moderation).

The "Act addressing terrorist content online" (TerrOIBG) was issued to fully comply with the European Regulation obligations throughout all of Germany. The Act assigned tasks to the Bundeskriminalamt and the Bundesnetzagentur for enforcing the Regulation.

The Bundeskriminalamt is responsible for issuing removal orders and drawing up removal requests as well as scrutinising removal orders addressed to German hosting service providers from authorities in other EU countries. Removal orders can also be addressed directly to hosting service providers in other EU countries. The Bundeskriminalamt consults with the North-Rhine Westphalian state media authority within the scope of its tasks on behalf of all the German state media authorities. In addition, the Bundeskriminalamt receives and deals with information on imminent threats to life as per Article 14(5) of the Regulation.

The Bundesnetzagentur's responsibility under the Act addressing terrorist content online is limited to hosting service providers that are based, or whose legal representatives are based, in Germany. The Bundesnetzagentur is responsible for all administrative fine proceedings under the Act, for instance whenever companies do not comply with the Bundeskriminalamt's removal orders. Furthermore, the Bundesnetzagentur takes the decision under Article 5(4) of the Regulation as to whether a hosting service provider is exposed to terrorist content online. Subsequently the Bundesnetzagentur monitors the specific measures taken by the respective hosting service provider. To ensure that removal orders actually reach the hosting service providers, they must establish a contact point pursuant to Article 15 of the Regulation and inform the Bundesnetzagentur of this.

Administrative fines may be imposed to enforce the administrative orders issued by the Bundeskriminalamt and the Bundesnetzagentur.

The data processing and communications system referred to as PERCI, which is used for transmitting removal orders and removal requests between national authorities, Europol and the hosting service providers, was put into operation by Europol on 3 July 2023 and is now being used by the majority of the Member States.

2. Transparency report/Monitoring report

Pursuant to Article 21(1) of the Terrorist Content Online Regulation and section 3 of the Act addressing terrorist content online, Member States collect information from their competent authorities and the hosting service providers under their jurisdiction on the actions they took under this Regulation in the previous calendar year and send the information to the Commission by 31 March each year.
In addition, the competent authorities publish transparency reports each year in accordance with Article 8(1) of the Regulation and section 4 of the Act on their activities falling under the scope of the Regulation.

As set out in Article 8(1) sentence 2 and Article 21(1) sentence 2 of the Regulation, the information should include as a minimum:

- the number of removal orders issued under Article 3 of the Regulation, specifying the number of removal orders subject to Article 4(1) of the Regulation, the number of removal orders scrutinised under Article 4, and information on the implementation of those removal orders by the hosting service providers concerned, including the number of cases in which terrorist content was removed or access thereto was disabled and the number of cases in which terrorist content was not removed or access thereto was not disabled, furthermore, how quickly the removal or disabling was carried out;
- the number of decisions taken in accordance with Article 5(4), (6) or (7) and information on the implementation of those decisions by the hosting service providers;
- the specific measures taken pursuant to Article 5, including the number of items of terrorist content which have been removed or access to which has been disabled and the speed of the removal or disabling;
- the number of access requests issued by competent authorities regarding content preserved by hosting service providers pursuant to Article 6;
- the number of complaint procedures initiated and actions taken by the hosting service provider pursuant to Article 10;
- the number of administrative or judicial review proceedings initiated against removal orders or decisions pursuant to Article 5(4) and (6) and the decisions taken by the competent authority in accordance with national law on any such proceedings;
- the number of decisions imposing penalties pursuant to Article 18 and a description of the type of penalty imposed.

2.1 Information from the Bundeskriminalamt

Removal orders

In 2025 the Bundeskriminalamt issued 245 removal orders under the Terrorist Content Online Regulation. The hosting service providers responded to the removal orders in 243 cases, which corresponds to an implementation rate of 99.2%. The Bundeskriminalamt issued 237 fewer removal orders in 2025 than in the previous year.

In 2025 the Bundeskriminalamt received 28 removal orders issued to German hosting service providers from bodies outside of Germany for legal assessment. The removal orders were not disputed on the German side. In the previous year 11 removal orders had been issued by bodies outside of Germany to German hosting service providers. In 2025 a total of 24 out of the 28 removal orders from bodies outside of Germany were issued to one German hosting service provider against which an administrative procedure under Article 5 of the Regulation is pending at the Bundesnetzagentur.

In 2025 the Bundeskriminalamt received objections to six removal orders. The removal orders were withdrawn.

Removal requests

The Bundeskriminalamt uses a legal instrument called a removal request, also called a referral, prior to issuing a removal order. Removal requests are not a binding call for action for hosting service providers under the Terrorist Content Online Regulation, rather they rely on voluntary cooperation. Removal requests generally relate to illegal or terrorist content, which usually also infringes the terms and conditions of a hosting service provider. In 2025 the Bundeskriminalamt notified hosting service providers of a total of 29,792 removal requests to remove or disable criminal online content voluntarily, 12,747 more than in the previous year. In 27,772 cases the content was found to have been removed or disabled. This represents an implementation rate of 93.2%, compared with 87.4% in the previous year.

Removal requests may be made to the respective hosting service provider by the Bundeskriminalamt or other police services. There is no obligation for removal requests to be processed around the clock (24/7). However, if the content notified is considered to be terrorist content online, the Bundeskriminalamt will check that the content has been removed or disabled after two working days and, where necessary, will issue a removal order. Apart from this general procedure, removal orders can also be issued directly without any prior removal request. Where a removal order is not issued, this might be because, for example, the removal request refers to content that has criminal implications but does not constitute terrorist content within the meaning of the Regulation, or the hosting service provider is based outside the EU, which makes it more difficult to apply the Regulation.

2.2 Information from the Bundesnetzagentur

The administrative procedure pursuant to Article 5 of the Terrorist Content Online Regulation against a German hosting service provider, which has been pending since 2023, was continued in 2025. In the view of the Bundesnetzagentur and of the Bundeskriminalamt, the measures taken are generally suitable for mitigating the dissemination of terrorist content online on the platform of the hosting service provider concerned. The effectiveness of the measures taken could not, however, be maintained at a high level. The Bundesnetzagentur and the Bundeskriminalamt again identified an increase in the dissemination of terrorist content online. The hosting service provider modernised and restructured the measures in place in order to increase effectiveness again and reduce dependencies. The Bundesnetzagentur is currently evaluating the effectiveness of the new measures.

In 2025 the Bundesnetzagentur issued a decision in accordance with Article 5(4) of the Regulation against another hosting service provider, thus initiating an administrative procedure under Article 5 of the Regulation against a hosting service provider whose legal representative is based in Germany. The Bundesnetzagentur found that the hosting service provider was exposed to terrorist content and required the hosting service provider to take measures to prevent terrorist content from being disseminated to the public using the hosting service provider's service. The hosting service provider reported to the Bundesnetzagentur on the specific measures that it had taken and that it intended to take. An assessment of the measures showed that the hosting service provider's specific measures as described in the report did not adequately comply with Article 5(2) and (3) of the Regulation. The Bundesnetzagentur subsequently issued a decision in accordance with Article 5(6) of the Regulation requiring the hosting service provider to take the necessary measures to ensure compliance with the legal requirements. A further report from the hosting service provider concerned is still pending.

In addition to these administrative procedures, other hosting service providers took measures in 2025 to prevent the dissemination of terrorist content online.

The following is a compilation of the specific measures taken by the hosting service providers surveyed.

Organisational measures:
- the use of conditions of use
- the use of general terms and conditions
- the use of Community Directives.

Technical measures:
- the use of automated systems to check user-generated content for terrorist content using lists of keywords (including phrases and figures of speech in various languages) as well as text, image and audio analysis
- the use of systems for the automated assignment of risk assessment to content
- the use of artificial intelligence systems for the automated verification of images
- the use of self-learning filter systems for text and image content
- the use of hashing or matching mechanisms to identify terrorist image or audio content that is already known to be such
- conducting proactive real-time scans as well as retroactive scans over the entire content catalogue
- the use of technical means to restrict the choice of usernames and URLs
- the disabling of email addresses from user accounts that have been removed to prevent them being used to

set up new accounts
- the use of systems to automatically identify the use of terrorist-motivated combinations of Unicode emojis and to mark these for manual moderation
- restricting the use of search functions within platforms, for example to prevent known terrorist content online being automatically suggested by an autocomplete function
- blocking links to third-party websites with terrorist content.

Manual measures:
- the use of content moderation teams composed of internal and external staff (also providing cover for other languages)
- the manual verification of content that has been assessed as high risk by an automated verification system
- evaluation of measures previously implemented and the identification of new trends in terrorist content online as well as any potential means of bypassing the measures implemented
- regular training for moderation teams
- the identification of account clusters with terrorist activities
- providing notification channels for users and third parties
- providing user moderation possibilities (eg the possibility to disable and/or report comments on the user's own content).

2.3 Information from the hosting service providers

Pursuant to section 3(2) of the Act addressing terrorist content online in conjunction with Articles 6, 10 and 21(1) sentence 2 points (c) and (d) of the Terrorist Content Online Regulation, hosting service providers are also subject to a reporting requirement to the Bundesnetzagentur.

From 1 January 2025 to 31 December 2025, hosting service providers received a total of five requests from competent authorities for access to data that had been removed or access to which had been disabled as a result of a removal order or specific measures pursuant to Article 3 or 5 of the Regulation, for the purposes of the prevention, detection, investigation and prosecution of terrorist offences or for administrative or judicial review proceedings.

In accordance with Article 10 of the Terrorist Content Online Regulation, hosting service providers must set up complaint mechanisms. These mechanisms allow content providers whose content has been removed or access to which has been disabled due to specific measures under Article 5 of the Regulation to submit a complaint concerning that removal or disabling, requesting the reinstatement of the content or access.
From 1 January 2025 to 31 December 2025 a total of 10,562 items of content were removed due to specific measures taken under Article 5 of the Regulation. During the same period, hosting service providers received 42 complaints from users against the removal of their content. As a result of these complaints, access to the content was reinstated in seven cases following an examination of the original decision.

3. Summary/outlook

In 2025 the Bundeskriminalamt and the Bundesnetzagentur identified terrorist content online on hosting services to a considerable extent and intervened accordingly. The hosting service providers in question have been cooperating with the Bundeskriminalamt and the Bundesnetzagentur and in the majority of cases they have responded to the Bundeskriminalamt's removal request by deleting content voluntarily, with the result that it has not been necessary to issue any removal orders. Where the Bundeskriminalamt transmits removal orders to hosting service providers via the PERCI tool set up by Europol, this runs smoothly overall.

In 2025 the Bundesnetzagentur pursued two administrative procedures under Article 5 of the Terrorist Content Online Regulation against hosting service providers that are based, or whose legal representatives are based, in Germany. Intervention by means of coercive or administrative fine proceedings has so far not been necessary. Hosting service providers are basically endeavouring to take effective measures to combat the dissemination of terrorist content online and to cooperate with the competent authorities. As a result, it can be stated that the implementation of the Regulation is having a positive effect on mitigating the dissemination of terrorist content online.

The Bundeskriminalamt and the Bundesnetzagentur are supporting German hosting service providers in implementing the Regulation. At the beginning of 2026 the Bundesnetzagentur and the Bundeskriminalamt held a joint information event for hosting service providers. It is planned to hold such events in future every two years with the aim of informing all hosting service providers about current developments and new hosting service providers about their obligations.

Publisher’s details

Publisher

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Tulpenfeld 4

53113 Bonn
Germany

Ordering address | Contact

Section 905 Addressing Terrorist Content Online, Data Regulation

Tulpenfeld 4

53113 Bonn
Germany

terroristische-onlineinhalte@bnetza.de

www.bundesnetzagentur.de

Tel. +49 (0)228 14-0

Last revised

March 2026

Text

Section 905 Addressing Terrorist Content Online, Data Regulation

bundesnetzagentur.de

x.com/BNetzA

social.bund.de/@bnetza

youtube.com/BNetzA