MICROSOFT TRANSPARENCY REPORT UNDER THE EU TERRORIST CONTENT REGULATION 2021 (EU TCR)

GENERAL INFORMATION (as of 31 Dec. 2022)

Microsoft takes seriously its responsibility to prevent terrorists and violent extremists from exploiting digital platforms, including by addressing images and videos on our hosted services that include terrorist or violent extremist content (TVEC). Our service terms prohibit illegal activities, and as specified in our Code of Conduct, we prohibit posting terrorist or violent extremist content. Examples of TVEC include content that aids in recruitment to a terrorist or violent extremist organization or encourages terrorist or violent extremist activities. Additional information on sources used to identify terrorist organizations is available on the Microsoft on the Issues blog.

Microsoft takes a balanced approach to addressing TVEC, and we collaborate with other multistakeholder partners – including the Global Internet Forum to Counter Terrorism (GIFCT) – to help inform our policies and practices. TVEC is prohibited on Microsoft platforms and services, and we have joined the Christchurch Call to Action as part of our commitment to addressing the abuse of technology to spread such content.

Microsoft is a founding member of the GIFCT and sits on the GIFCT Operating Board. Via the GIFCT, Microsoft participates in a range of activity, including engagement in its multistakeholder working groups and the GIFCT's Incident Response processes. For further information, reference the GIFCT's annual transparency report, which includes information on the hash-sharing database.

Microsoft also provides transparency to the public about the actions it takes on its services to address TVEC in its Digital Safety Transparency Report (https://www.microsoft.com/en-us/corporate-responsibility/digital-safety-content-report). Additional information about safety specifically on our gaming services is available in the Xbox transparency report (https://www.xbox.com/en-US/legal/xbox-transparency-report).

In accordance with Regulation (EU) 2021/784, Microsoft provides the following report on actions taken to address the dissemination of terrorist content for the period January–December 2022.

a. Information about measures in relation to identification and removal of or disabling of access to Terrorist Content.

The Microsoft Services Agreement Code of Conduct prohibits the "posting [of] terrorist or violent extremist content." We encourage the reporting of content posted by – or in support of – a terrorist organization that depicts graphic violence, encourages violent action, endorses a terrorist organization or its acts, or encourages people to join such groups. We review these reports; take action on content; and, if necessary, take action on accounts associated with violations of our Code of Conduct. In addition, we leverage a variety of tools, including hash-matching technology and other forms of proactive detection, to detect TVEC.

As a GIFCT member (as outlined above), Microsoft participates in the GIFCT's Incident Response processes, including ingesting hashes related to an event activated as Content Incidents or Content Incident Protocols. This allows Microsoft to quickly become aware of, assess, and address potential content circulating online resulting from a terrorist or violent extremist event. For further information, reference the GIFCT's annual transparency report, which includes information on the hash-sharing database.

b. Information about measures used to address the reappearance online of material which has previously been removed or to which access has been disabled because it was considered to be Terrorist Content, in particular where automated tools have been used.

Microsoft leverages hash-matching technology to address the reappearance online of content that has been previously identified as Terrorist Content in violation of

Microsoft's policies. Hash-matching technology uses a mathematical algorithm to create a unique signature (known as a "hash") for digital images and videos. The hashing technology then compares the hashes generated from user-generated content (UGC) with hashes of reported (known) Terrorist Content, in a process called "hash matching".

c. The number of items of Terrorist Content removed or to which access has been disabled, pursuant to removal orders issued under the TCR, and the number of removal orders under the TCR where the content has not been removed or access to which has not been disabled, together with the grounds therefor.

   Microsoft received zero removal orders under the EU TCR during the reporting period.

d. Number of complaints from content providers requesting reinstatement of Terrorist Content removed or to which access has been disabled by Microsoft.

   In 2022, Microsoft received and closed 64 complaints from content providers requesting reinstatement of Terrorist Content removed or to which access has been disabled in the European Union.

e. The number and outcome of administrative or judicial review brought by the hosting service provider.

   Microsoft received zero removal orders under the EU TCR during the reporting period. As a result, there were zero administrative or judicial reviews brought by Microsoft during the reporting period.

f. The number of cases in which the hosting service provider was required to reinstate content or access thereto as a result of administrative or judicial review proceedings.

Microsoft received zero removal orders under the EU TCR during the reporting period. As a result, there were zero cases in which Microsoft was required to reinstate content or access thereto as a result of administrative or judicial reviews proceedings during the reporting period.

g. The number of cases in which the hosting service provider reinstated Terrorist content or access thereto following a complaint by the content provider.

Microsoft reinstated Terrorist Content or access thereto in zero cases following a complaint by the content provider in the European Union during the reporting period.