Microsoft Transparency Report under the EU Terrorist Content Regulation 2021 (EU TCR)

GENERAL INFORMATION (as of 31 Dec. 2023)

Microsoft takes seriously its responsibility to prevent terrorists and violent extremists from exploiting digital platforms, including by addressing terrorist or violent extremist content (TVEC) on our hosted consumer services. As specified in Microsoft's Code of Conduct and on our Digital Safety site, we do not allow content that praises or supports terrorists or violent extremists, helps them to recruit, or encourages or enables their activities. We look to the United Nations Security Council's Consolidated List to identify terrorists or terrorist groups. Violent extremists include people who embrace an ideology of violence or violent hatred towards another group.

Microsoft's approach to addressing TVEC is consistent with our responsibility to manage our services in a way that respects fundamental values such as safety, privacy, and freedom of expression. We collaborate with multistakeholder partners – including the EU Internet Forum, the Global Internet Forum to Counter Terrorism (GIFCT) and the Christchurch Call to Action to work collectively to eliminate terrorist and violent extremist content online.

Microsoft is a founding member of the GIFCT and, in 2024, holds the Chair of the GIFCT Operating Board. Via GIFCT, Microsoft participates in a range of activity, including GIFCT's Incident Response processes. In the event the GIFCT activates a Content Incident or Content Incident Protocol, Microsoft ingests related hashes from GIFCT's hash-sharing database. This allows Microsoft to quickly become aware of, assess, and address content circulating on its hosted consumer services resulting from an offline terrorist or violent extremist event consistent with Microsoft policies. For further information, reference 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) and its Digital Safety site. 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 2023.

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

As specified in Microsoft's Code of Conduct and on our Digital Safety site, we do not allow content that praises or supports terrorists or violent extremists, helps them to recruit, or encourages or enables their activities. We look to the United Nations Security Council's Consolidated List to identify terrorists or terrorist groups. Violent extremists include people who embrace an ideology of violence or violent hatred towards another group. We review reports from users and third parties on potential TVEC, 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 for subsequent review.

As a GIFCT member (as outlined above), Microsoft participates in 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 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 2023, Microsoft received and closed 21 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.