MICROSOFT TRANSPARENCY REPORT (REGULATION (EU) 2021/1232)

GENERAL INFORMATION (as of Dec. 31, 2021)

Microsoft takes seriously its responsibility to prevent child sexual exploitation and abuse imagery (CSEAI) from distribution through its services. Our service terms prohibit illegal activities, and as specified in our Code of Conduct, we prohibit activities that exploit, harm, or threaten to harm children.

Microsoft has a longstanding commitment to participating in multi-stakeholder approaches to prevent the spread of CSEAI. Its efforts include the development of PhotoDNA (https://www.microsoft.com/en-us/photodna), a technology it has shared with organizations around the world to fight CSEAI.


Pursuant to Article 3, Subsection (g)(vii) of Regulation (EU) 2021/1232, Microsoft provides the following report on its data processing activities specific to Microsoft Number-Independent Interpersonal Communications Services [NI-ICS] in connection with the use of technology to detect CSEAI for the period July-December 2021.

1. Type and volumes of data processed during the reporting period
   a. Over 8.9 billion content items scanned, globally.

2. Specific ground relied on for the processing pursuant to Regulation (EU) 2016/679
   a. Varies based on processing, including public interest under GDPR Article 6(1)(e).

3. The ground relied on for transfers of personal data outside the European Union pursuant to Chapter V of Regulation (EU) 2016/679, where applicable
   a. Varies based on transfer, including standard contractual clauses under GDPR Article 46(2)(c).

4. Number of cases of online child sexual abuse identified
a. Over 20,000 content items confirmed as CSEAI globally in NI-ICS during the period, with over 6,600 of those content items detected from the European Union.

5. Number of cases in which a user has lodged a complaint with the internal redress mechanism or with a judicial authority, and the outcome of such complaints
   a. Microsoft tracks customer contacts to its privacy team and EU Data Protection Officer where its data processing activities in connection with the use of technology to detect CSEAI are at issue. Civil litigation involving these activities, and their impact on the customer, would also be tracked. During the period July – December 2021, Microsoft tracked zero complaints for the European Union that address the use of this technology in NI-ICS.

6. Number and ratios of errors (false positives) of the different technologies used
   a. Microsoft uses hash-matching technology (including PhotoDNA and MD5 hashing) to detect known CSEAI imagery shared through NI-ICS. Hash-matching technology works by using 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) CSEAI, in a process called "hash matching".

   b. Microsoft implements a layered approach to detection of CSEAI through NI-ICS combining both hash-matching technology and manual review. During the reporting period, Microsoft tracked zero false positives for CSEAI detection, defined as enforcement decision reversals, in NI-ICS. This number is representative of Microsoft’s implementation of hash-matching technology.

7. Measures applied to limit the numbers and ratios of errors (false positives) of the different technologies used
   a. Microsoft implements our own hash verification process in which Microsoft trained analysts review and confirm images associated with hashes provided from non-profits and other industry partners. Microsoft also leverages an additional manual review process as an ongoing hash quality check.

8. The retention policy and data protection safeguards applied pursuant to Regulation (EU) 2016/679
   a. Data retention varies depending on the type of data, but in each case the retention period is limited to the time appropriate for the type of data and the purpose of processing. Data will be deleted at the end of the retention period. Data minimization and protection efforts include de-identification
or pseudonymization techniques (e.g., masking, hashing, differential privacy). Privacy reviews are conducted to identify, assess, and mitigate potential privacy risks from the collection, processing, storing, and sharing of personal data when new system capabilities or processes are being designed. Finally, Microsoft minimizes the data involved in the scanning process by hashing it.

9. The names of organizations acting in the public interest against child sexual abuse with which data has been shared
   a. The U.S. National Center for Missing and Exploited Children (NCMEC). According to NCMEC’s official statement, NCMEC staff review each report and work to find a potential location for the incident reported so that it may be made available to the appropriate law-enforcement agency for possible investigation.
Microsoft Response to European Commission questions regarding: MICROSOFT TRANSPARENCY REPORT (REGULATION (EU) 2021/1232)

1. **Types and volumes of data processed:** Please specify the types of **content data** (text, images, video, other) and **traffic data** (persons involved in communications or their identifiers, their location, date and time of communications, other) **processed and the respective volumes** (in GB or number of data sets) of the different types of content and traffic data processed.

   The transparency report was scoped to the services impacted by and the content at issue in EU Regulation 2021/1232, that is: Microsoft’s number-independent interpersonal communications services (NI-ICS) scanning for CSAM such as Outlook.com and Skype. None of the services referenced in the transparency report conducts text scanning to identify solicitation activities.

   Content types scanned for CSAM are images and videos. Microsoft relies on the hash matching technologies PhotoDNA and MD5 to detect matches of previously identified CSAM. Note, the hashes themselves contain no data about the user or image that caused the hash to be created.

   Traffic data Microsoft collects is included in its Cybertip reports to the National Center for Missing and Exploited Children (NCMEC). This data includes the following items:
   1. User id (i.e., Microsoft Account ID) and username;
   2. Event timestamp; and
   3. IP address.

   From July to December 2021, Microsoft scanned approximately 8.9 billion images and 51 million videos globally, detecting approximately 6,600 content items shared from the European Union identified as CSEAI for the services referenced in the transparency report. Microsoft made approximately 4,500 Cybertip reports related to those content items.

2. **a.** In the heading of your responses to the questions you use the term ‘child sexual exploitation and abuse imagery (CSEAI)’. Could you please **clarify whether this term covers only ‘online child sexual abuse material’ or also ‘solicitation of children’**, as defined in Article 2(2), 2(3) of Regulation (EU) 2021/1232?

   **b.** On question 1 regarding the type and volumes of data processed during the reporting period, you mention that over 8.9 billion ‘content items’ were scanned, globally. Could you please also report the number at the EU level? Could you please explain what the term ‘content item’ means in practice? Could you please indicate what types of data processed (for instance emails, messages, videos, images, other) and how many of the different types?

   **c.** Regarding question 5, could you please inform if the number of zero complaints for the EU covers internal redress mechanisms (Microsoft’s privacy team) or complaints lodged with a supervisory authority?
2(a) For purposes of this report “CSEAI” or child sexual exploitation and abuse imagery, includes text and imagery of child sexual abuse as defined by Microsoft’s policies. It does not include “solicitation of children” as none of the services referenced in the transparency report conducts scanning to identify such activities.

2(b) The number of content items scanned was not tracked at a country or regional level, and as such an EU-specific count is unavailable to Microsoft. Microsoft is actively working on its data tracking methodologies to ensure datasets can be tracked at a country and region level in the future. For the purposes of this report, ‘content item’ means a single image or video. Please refer to the answer to question #1 regarding types of data processed.

2(c) During the period July to December 2021, Microsoft received zero complaints to its internal privacy team or from supervisory authority in Europe in relation to its CSAM scanning in the EU on the services referenced in the transparency report.

3. On question 6 regarding the number and ratios of errors (false positives) of the different technologies used, you report only on the use of hashing technology and you state that during the reporting period Microsoft tracked zero false positives for CSEAI detection. However, the link contained in the heading of the Report also contains information on grooming. Could you please clarify this point? In the event that grooming is also covered could you please clarify the relationship between the false positives statistics and the Digital Safety Content Report findings?

The Transparency Report required under EU Regulation 2021/1232 is a subset of Microsoft’s Digital Safety Content Report.

Microsoft’s Digital Safety Content Report covers more services, content categories, and content types than those which are referenced in the Transparency Report required under EU Regulation 2021/1232. The false positive statistics disclosed in the Transparency Report relate only to the services and content covered within the Transparency Report and PhotoDNA/MD5 hash matching for CSAM on those services. None of those services conducts scanning activities for purposes of detecting solicitation, or grooming and as such, statistics related to false positives for such scanning are inapplicable to the activities described in the Transparency Report.

4. Have you received any feedback on the number of errors (false positives), from the organisations with which the data has been shared?

We share data through Cybertips to NCMEC and with law enforcement subject to lawful process. While we received trend data from NCMEC, we did not receive feedback from NCMEC or law enforcement related to false positives occurring in relation to content found on the referenced services between July and December 2021.
5. On question 8 regarding the retention policy, could you please clarify the data retention periods or at least the criteria used to determine them?

Once content has been verified by Microsoft as CSAM through human review, a copy of the image or video is placed in secure storage managed by Microsoft’s Law Enforcement and National Security team and retained for 90 days. If the content detected was content hosted by Microsoft through a Microsoft Account, the content is deleted from the account.

The storage system automatically deletes the stored CSAM content after 90 days unless the storage period has been extended upon receipt of lawful process, generally related to law enforcement agencies following up on NCMEC reports. Any non-CSAM contents of relevant accounts are retained in accordance with retention practices for those services, including retention practices for suspended accounts as detailed in the Microsoft Services Agreement. These retention periods vary depending on the type of data, but in each case the retention period is limited to the time appropriate for the type of data and the purpose of processing.

More information about Microsoft’s retention practices is available through the Microsoft Privacy Statement, which states that:

*Microsoft retains personal data for as long as necessary to provide the products and fulfil the transactions you have requested, or for other legitimate purposes such as complying with our legal obligations, resolving disputes, and enforcing our agreements. Because these needs can vary for different data types, the context of our interactions with you or your use of products, actual retention periods can vary significantly.*

*Other criteria used to determine the retention periods include:*

- Do customers provide, create, or maintain the data with the expectation we will retain it until they affirmatively remove it? Examples include a document you store in OneDrive, or an email message you keep in your Outlook.com inbox. In such cases, we would aim to maintain the data until you actively delete it, such as by moving an email from your Outlook.com inbox to the Deleted Items folder, and then emptying that folder (when your Deleted Items folder is emptied, those emptied items remain in our system for up to 30 days before final deletion). (Note that there may be other reasons why the data has to be deleted sooner, for example if you exceed limits on how much data can be stored in your account.)
- Is there an automated control, such as in the Microsoft privacy dashboard, that enables the customer to access and delete the personal data at any time? If there is not, a shortened data retention time will generally be adopted.
- Is the personal data of a sensitive type? If so, a shortened retention time would generally be adopted.
- Has Microsoft adopted and announced a specific retention period for a certain data type? For example, for Bing search queries, we de-identify stored queries by
removing the entirety of the IP address after 6 months, and cookie IDs and other cross-session identifiers that are used to identify a particular account or device after 18 months.

- Has the user provided consent for a longer retention period? If so, we will retain data in accordance with your consent.
- Is Microsoft subject to a legal, contractual, or similar obligation to retain or delete the data? Examples can include mandatory data retention laws in the applicable jurisdiction, government orders to preserve data relevant to an investigation, or data retained for the purposes of litigation. Conversely, if we are required by law to remove unlawful content, we will do so.