MICROSOFT EUROPEAN UNION CHILD SEXUAL ABUSE MATERIAL INTERIM REGULATORY REPORT (JANUARY-DECEMBER ‘25)

Microsoft

Table of Contents

Microsoft

Microsoft Transparency Report (Regulation (eu) 2021/1232)

General Information (as of 31 Dec. 2025)

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.

Microsoft also provides transparency to the public about the actions it takes on its services to address CSEAI in its Digital Safety Transparency Report (https://www.microsoft.com/en-us/corporate-responsibility/digital-safety-content-report).

Microsoft

In accordance with 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 January to December 2025.

1. Type and volumes of data processed during the year-long reporting period

a. Microsoft's transparency report is 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) that use technology for detection of CSEAI as described below.
    i. Outlook.com

b. Traffic data Microsoft collects is included in its CyberTip reports to the U.S. National Center for Missing and Exploited Children (NCMEC). This data includes the following items:
    i. User ID (i.e., Microsoft Account ID) and username;
    ii. Event timestamp; and
    iii. IP address.

c. Content types scanned for CSEAI are images and videos. Microsoft relies on the hash matching technologies PhotoDNA and MD5 to detect matches of previously

identified CSEAI. Note, the hashes themselves contain no data about the user or image that caused the hash to be created.

	EU Users	Non-EU Users	Global
# of Images Processed	No geo data for scanned content	No geo data for scanned content	13,734,449,620
# of Videos Processed	No geo data for scanned content	No geo data for scanned content	0
# of Other Files Processed[1]	No geo data for scanned content	No geo data for scanned content	1,556,208,199
# of Bytes of Text Processed	NA	NA	NA

Other information of relevance to the types and volumes of data processed:

i. The quantitative figures provided for the numbers of images, videos, and other files processed reflect global volumes across Outlook. Microsoft does not maintain geo-segmented metrics that distinguish EU users from non-EU users for scanned content used in the detection of child sexual abuse material. As a result, it is not possible to attribute these volumes specifically to EU users. Where applicable, this limitation is reflected in the tables above.

ii. Microsoft did not process text data under Regulation (EU) 2021/1232, and no additional categories of data or processing activities beyond those described above were performed for the purposes of CSEAI detection during the reporting period.

[1] Types of files:
- Global Users

2. Specific ground relied on for the processing pursuant to Regulation (EU) 2016/679

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

Varies based on transfer, including standard contractual clauses under GDPR Article 46(2)(c). Microsoft is also certified to the EU-U.S. and Swiss-U.S. Data Privacy Frameworks and the commitments they entail.

4. Number of cases of online child sexual abuse identified

a. Known CSAM

	EU Users
# of Reports	0
# of Images	0
# of Videos	0
# of Other Files	0
# of User Accounts Sending	183
# of User Accounts Receiving	0

b. New CSAM

Microsoft does not deploy classifiers or other technologies capable of detecting previously unknown child sexual abuse material. Accordingly, Microsoft did not identify,

process, or report possible new CSAM during the reporting period, and all metrics in this section are not applicable.

	EU Users
# of Reports	NA
# of Images	NA
# of Videos	NA
# of Other Files	NA
# of User Accounts Sending	NA
# of User Accounts Receiving	NA

c. Solicitation

Microsoft does not scan for the purpose of detecting the solicitation of children. Accordingly, Microsoft did not generate reports, flag user accounts, suspend user accounts, or process related data for solicitation detection during the reporting period, and all metrics in this section are not applicable.

	EU Users
# of Reports	NA
# of User Accounts Sending	NA
# of User Accounts Receiving	NA

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. Known CSAM

No complaints were lodged with either the internal redress mechanism or a judicial authority during the reporting period. As no complaints were received, optional time to decision metrics are not applicable.

i. Content Items

# of items removed	0
# of complaints lodged w/ the internal mechanism	0
# of items removed, but restored (internal mechanism)	0
# of complaints lodged w/ the judicial authority	0
# of items removed, but restored (judicial authority)	0

ii. User Accounts in the EU

# of user accounts suspended	0
# of complaints lodged w/ the internal mechanism	0
# of user accounts suspended, but restored (internal mechanism)	0
# of complaints lodged w/ the judicial authority	0
# of accounts suspended, but restored (judicial authority)	0

b. New CSAM

Microsoft does not deploy classifiers or other technologies capable of detecting previously unknown child sexual abuse material. Accordingly, Microsoft did not identify, process, or report possible new CSAM during the reporting period, and all metrics in this section are not applicable.

i. Content Items

# of items removed	NA
# of complaints lodged w/ the internal mechanism	NA

# of items removed, but restored (internal mechanism)	NA
# of complaints lodged w/ the judicial authority	NA
# of items removed, but restored (judicial authority)	NA

ii. User Accounts in the EU

# of user accounts suspended	NA
# of complaints lodged w/ the internal mechanism	NA
# of user accounts suspended, but restored (internal mechanism)	NA
# of complaints lodged w/ the judicial authority	NA
# of accounts suspended, but restored (judicial authority)	NA

c. Solicitation

Microsoft does not scan for the purpose of detecting the solicitation of children. Accordingly, Microsoft did not generate reports, flag user accounts, suspend user accounts, or process related data for solicitation detection during the reporting period, and all metrics in this section are not applicable.

i. User Accounts in the EU

# of user accounts suspended	NA
# of complaints lodged w/ the internal mechanism	NA
# of user accounts suspended, but restored (internal mechanism)	NA
# of complaints lodged w/ the judicial authority	NA
# of accounts suspended, but restored (judicial authority)	NA

6. Number and ratios of errors (false positives) of the different technologies used

a. Known CSAM

	Global
# of content items automatically flagged	1127
# of content items automatically flagged which are not known CSAM upon human review	173
Error Rate	15.35%
# of content items automatically flagged as constituting known CSAM that are subject to human review	1092

Other relevant findings:

i. The quantitative figures reported in this section reflect global calculations of error rates for the relevant detection technologies and are not limited to EU users. Microsoft does not maintain error rate metrics segmented by user geography for these technologies. Accordingly, the figures presented are provided to explain the operation and effectiveness of the detection technologies generally rather than EU specific metrics.

ii. Error code B1 / C1: The percentage of content items automatically flagged as constituting known CSAM that were determined not to be CSAM upon human review, out of those automatically flagged and subject to human review was 15.84%. These figures reflect global Outlook.com data and are not geo-segmented.

b. New CSAM

Microsoft does not deploy classifiers or other technologies capable of detecting previously unknown child sexual abuse material. Accordingly, Microsoft did not identify, process, or report possible new CSAM during the reporting period, and all metrics in this section are not applicable.

# of content items automatically flagged	NA
# of content items automatically flagged which are not CSAM upon human review	NA
Error Rate	NA
# of content items automatically flagged as constituting new CSAM that are subject to human review	NA

Other relevant findings: NA

c. Solicitation (in EU)

Microsoft does not scan for the purpose of detecting the solicitation of children. Accordingly, Microsoft did not generate reports, flag user accounts, suspend user accounts, or process related data for solicitation detection during the reporting period, and all metrics in this section are not applicable.

# of user accounts automatically flagged	NA
# of user accounts automatically flagged which were not involved in solicitation upon human review	NA
Error Rate	NA
of user accounts in the EU automatically flagged as either having solicited a child or being solicited as a child that are subject to human review	NA

Other relevant findings: NA

7. Measures applied to limit the numbers and ratios of errors (false positives) of the different technologies used

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.

a. Known CSAM

i. Indicators

Microsoft implements our own hash verification process in which Microsoft-trained analysts review images that generate hash hits as we encounter them in the course of business and confirm whether hashes provided from non-profits or other industry partners identify CSAM images. A hash cannot be vetted before it is added to the database since hashes are not reversible and, therefore, cannot be reviewed. Microsoft initially marks externally provided hashes that it adds to its database as "untrusted".

ii. Implementation of the Detection Technology

If and when Microsoft encounters content that matches such hashes the content is reviewed by Microsoft-trained reviewers and the outcome of that review will determine whether future hits should be treated as indicative of violative content or non-violative content. When Microsoft makes updates to our hash matching code, such as adding support for new platforms or making performance improvements, we run the updated algorithms on a corpus of test data to ensure that the outcome of the hash calculations and distance calculations are unchanged.

iii. Human Review

Microsoft performs human review on a cross section of hash hits, including hashes that have been previously hit, and analyzes the results to ensure that the overall accuracy of the hash set remains at acceptable levels.

iv. Other Measures

When it is discovered that a particular hash has a tendency to flag non-violative content, such hashes are removed from the system. Microsoft also leverages an additional manual review process as an ongoing hash quality check.

v. Error Rate

The error rate for known CSAM reflects the proportion of content items automatically flagged by hash-matching technologies that are determined not to constitute known child sexual abuse material following human review. The error rate reported in this section is calculated based on these review outcomes and is presented in Section 6.

b. New CSAM

i. Indicators

Microsoft does not deploy classifiers capable of detecting previously unknown CSAM. Accordingly, no indicators are applicable.

ii. Implementation of the Detection Technology

Not applicable, as no detection technology for new CSAM is deployed.

iii. Human Review

Not applicable.

iv. Other Measures

Not applicable.

v. Error Rate

Not applicable, as no detection occurs.

c. Solicitation

i. Indicators

The in-scope services do not scan to detect grooming or solicitation of children. Accordingly, no indicators apply for this category.

ii. Implementation of the Detection Technology

Microsoft does not deploy detection technologies to identify grooming or solicitation of children for the in-scope services. As a result, no implementation measures apply.

iii. Human Review

Not applicable.

iv. Other Measures

Not applicable.

v. Error Rate

As the in-scope services do not scan to detect grooming or solicitation of children, no error rate is applicable for this category.

8. The retention policy and data protection safeguards applied pursuant to Regulation (EU) 2016/679

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.

a. Retention Policies

The Digital Trust and Safety (DigiTS) Team operates in accordance with Microsoft's enterprise-wide privacy, security, and data governance framework, including the Microsoft 365 (M365) compliance programs. The M365 Trust Privacy program ensures service teams have retention policies in place to govern data handling per data type. Retention policies for non-content data related to reports of online CSA are broken out to relevant data type and defined appropriately. Retention policies for data related to complaints and policy violations are broken out by relevant data type and defined appropriately.

b. Data Protection Safeguards

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. Microsoft encrypts data in transit using industry-standard secure communication protocols. Encryption applies to data in transit and is governed by Microsoft's enterprise security standards. Where feasible, personal data is minimized, anonymized, pseudonymized, or otherwise de-identified

to reduce privacy risk while supporting legitimate business and safety purposes. Microsoft maintains enterprise-wide security incident response plans and procedures designed to monitor, detect, investigate, and remediate potential security vulnerabilities and incidents across its infrastructure. Security monitoring is continuously performed through automated detection capabilities, centralized logging, and alerting mechanisms. Identified security events are triaged and assessed by dedicated security teams in accordance with established incident management processes. Security monitoring is continuously performed through automated detection capabilities, centralized logging, and alerting mechanisms to identify potential threats or anomalous activity. Identified security events are triaged and assessed by dedicated security teams in accordance with established incident management processes.

9. The names of organizations acting in the public interest against child sexual abuse with which data has been shared

Microsoft reports apparent CSAM to the U.S. National Center for Missing and Exploited Children (NCMEC).