

PikPak Transparency Report

Period ending 30 June 2025

Report issued 29th August 2025

1. Introduction

The transparency report provides a clear overview of PikPak's operations, reflecting our commitment to accountability and user safety. This report is published in accordance with the **EU Digital Services Act (DSA)** ^[1] and other relevant government and industry policies, aiming to keep users, regulators, and stakeholders informed about our content moderation, data handling, user protection, and other key practices. All statistical data in this report is anonymized and does not include any personally identifiable user information.

This is the **first transparency report** since PikPak commenced operations in July 2021, covering the **one-year period from 1 July 2024 to 30 June 2025**. PikPak intends to provide **regular transparency updates in future reports**.

We are committed to fostering a safe and secure online environment and recognize our responsibility to protect both individual privacy and the wider internet community. Within this framework of responsibility, PikPak enforces a strict **zero-tolerance policy against all forms of illegal content, such as Child Sexual Abuse Material (CSAM)**.

2. Industry Cooperation

PikPak is an active member of the **Internet Watch Foundation (IWF)**, an international organisation dedicated to identifying and removing online child sexual abuse imagery. Through this collaboration, PikPak contributes to global efforts to detect, report, and remove harmful material, working closely with industry partners, regulatory bodies, and law enforcement agencies.

To support its cooperation with the IWF, PikPak employs an **automated hash-matching system** to detect and block known CSAM. Stored files are regularly scanned and compared against the IWF's CSAM hash list. When a match is identified, the file is automatically blocked from access or

sharing. This process demonstrates high accuracy, with no significant false positives or false negatives recorded. For more information on the IWF, please visit: <https://www.iwf.org.uk>.

3. Regulatory Background

PikPak follows clear compliance procedures to address unlawful content, including illegal material and copyright infringement. Files stored privately in user accounts are not subject to proactive review.

When a user generates a sharing link, anyone with that link (and optional password) can view, save, download, and further share the file or folder. Compliance reviews are initiated only in connection with such shared content.

Privately stored files remain outside the scope of proactive monitoring, except where legal obligations apply. In limited circumstances, such as valid requests from judicial or law enforcement authorities regarding confirmed illegal activity, PikPak may review or disclose user data strictly in accordance with applicable law.

4. PikPak Policies

Privacy Policy

PikPak is committed to protecting user privacy and securing personal information.

Data is collected and used only as necessary to provide our services, improve user experience, and ensure account security. Personal information is disclosed only when required by law or a lawful request from competent authorities.

Personal data is retained only for the minimum period necessary to fulfill the purposes described or as required by law. Once it is no longer needed, the data is securely deleted or anonymized so that it can no longer be linked to any individual. During the retention period, all personal data is protected with strict safeguards, and users retain the right to access, correct, or delete their information at any time. Data associated with closed accounts is promptly removed or anonymized in accordance with applicable laws and our policies, as set out in the [PikPak Privacy Policy](#).

Copyright

PikPak's [User Agreement](#) and [Copyright Infringement Policy](#) expressly prohibit users from using our services to infringe copyright or other intellectual property rights.

If copyright holders discover that their protected works are being stored, shared, or accessed via PikPak's services without authorisation, they may submit a copyright notice to us. PikPak will process such requests in accordance with applicable laws and our policies, removing or restricting access to infringing material as required.

In line with applicable copyright laws, PikPak benefits from safe harbour protection, which shields the platform from direct liability for content uploaded and shared by users. Although PikPak is not legally bound by U.S. or EU law, we follow the principles of the U.S. Digital Millennium Copyright Act (DMCA) and relevant European Union directives by implementing a notice-and-takedown system.

PikPak's commitment is to **process takedown requests expeditiously** and ensure efficient responses to rights holders.

Illegal Content

Under the [User Agreement](#), [Anti-Abuse Policy](#), and [Child Sexual Abuse Policy](#), PikPak strictly prohibits the upload, storage, or sharing of the following categories of illegal content, including but not limited to:

- Child Sexual Abuse Material (CSAM)
- Violent extremism content
- Content in violation of applicable laws and regulations

PikPak maintains a **zero-tolerance policy** for **CSAM**. Users, law enforcement authorities, and members of the public may report such content to abuse@mypikpak.com.

If, however, we are made aware that our services have been used to store and/or transmit any such illegal content, PikPak acts immediately to remove all such content, block the user accounts involved, and report all related activity to the authorities. PikPak hereby reserves the

right to take further action, including but not limited to cooperation with law enforcement agencies and/or government bodies to assist them in prosecuting those involved.

5. Copyright Matters

PikPak's approach to dealing with requests for the takedown of content uploaded by its users is set out in its [Copyright Infringement Policy](#).

PikPak accepts copyright takedown notices via a [dedicated web page](#) or by email to copyright@mypikpak.com.

PikPak reviews all copyright complaints to ensure their validity before taking action. Verified complaints result in the immediate **blocking of the reported share links**, preventing any user from accessing or saving the associated content. Links containing copyrighted content, even if they include multiple files, are **blocked** when reported, ensuring unauthorized access is prevented. Most copyright reports are resolved within **6 hours**, and cases requiring further review are completed within **3 days**.

Overall, the number of verified takedown requests represents a **small fraction of the total content stored** on PikPak.

Period	Valid Copyright Complaints Received	Copyright Links Actioned	Percentage of Total Links (%)
1 Jul 2024 – 30 Jun 2025	832	3683	0.024

Table 1– Copyright takedowns.

6. Counter-Notices

PikPak respects the legitimate interests of both copyright owners and users. In addition to processing takedown notices, PikPak provides a **counter-notice mechanism** for users whose content may have been removed by mistake or misidentification.

Under our [Copyright Infringement Policy](#), users may submit a counter-notice including their signature, identification of the removed material and its original location, a good-faith statement under penalty of perjury, contact details, and a statement of consent to jurisdiction. Counter-notices may be submitted via [dedicated web page](#) or through PikPak's designated agent.

If the counter-notice is compliant, PikPak will restore access to the material within **10 to 14 business days**, unless the original complainant informs PikPak that legal proceedings have been initiated against the user.

In practice, however, due to the careful review process we apply before removing content in response to infringement notices, there have not yet been any cases where material was reinstated through the counter-notice mechanism.

This outcome demonstrates that PikPak's copyright notice and takedown system is functioning effectively, with very low levels of misuse. We remain committed to maintaining a fair and balanced approach that protects the rights of copyright owners while safeguarding legitimate user interests.

7. Illegal Content

To date, PikPak has taken decisive enforcement measures against accounts involved in uploading or distributing illegal content.

Illegal content is categorised as follows. As shown in the chart below, reports and confirmed violations related to CSAM account for **99.93%** of all cases. A smaller proportion of cases involved **terrorism and violent extremism (0.05%)**, **non-consensual image sharing (0.02%)**, and **other forms of illegal content (0.01%)**.

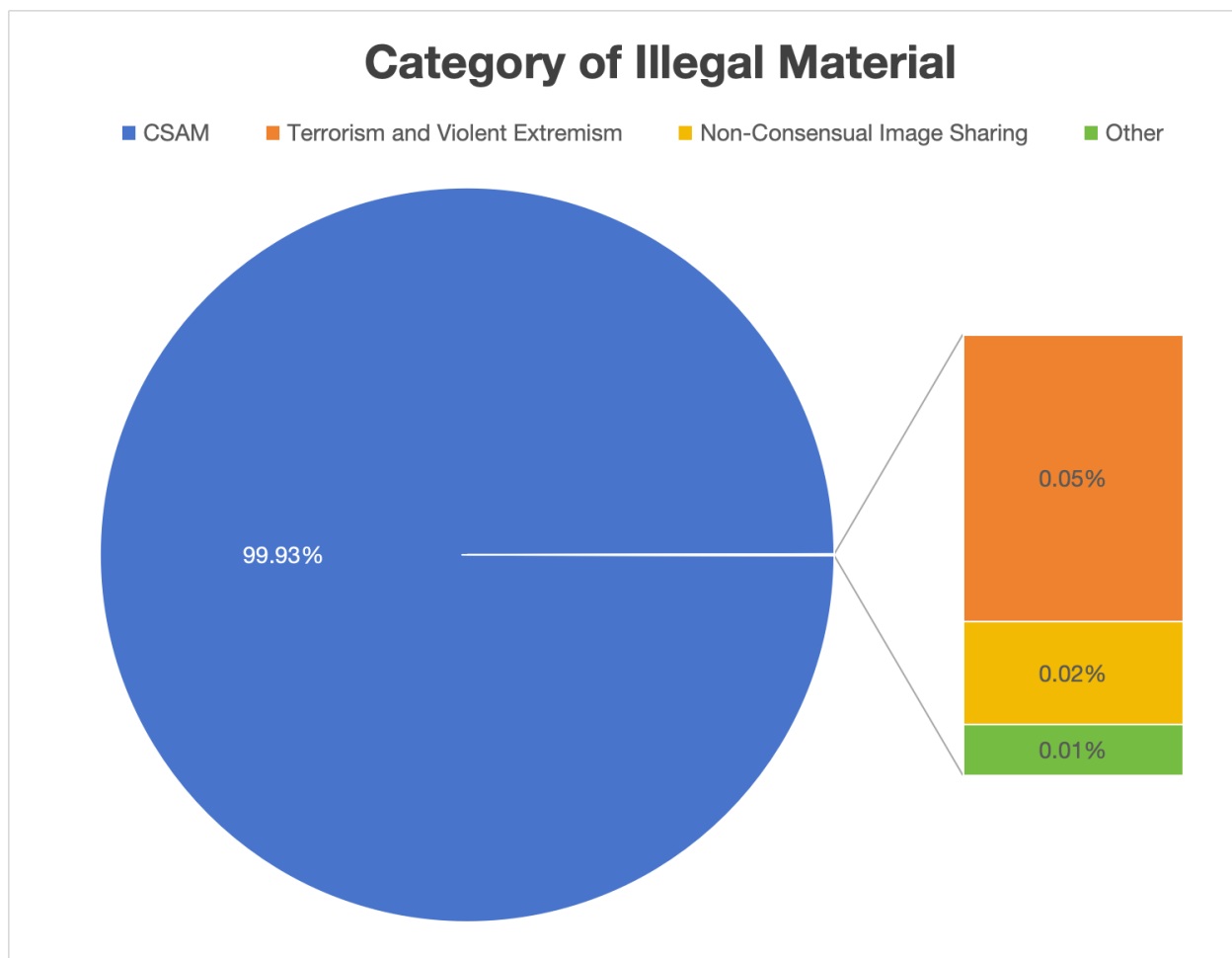


Figure 1 - Reports of illegal material mainly concern CSAM, with a small number involving other serious crimes.

As illustrated in Figure 1, CSAM accounts for the largest proportion of detected illegal content, consistent with reports from other platforms. We treat this issue with the utmost seriousness and have implemented comprehensive measures to detect, block, and prevent the dissemination of such material in accordance with our policies and applicable laws.

8. Identification of Illegal Content

PikPak employs a combination of **proactive detection** and **multiple reporting channels** to address illegal content. Proactive measures apply only to files that users choose to share, ensuring that privately stored files remain unaffected. Files already confirmed as CSAM are blocked from being uploaded, cloud downloaded, or shared.

The majority of CSAM removals result from proactive detection before any report is received. PikPak regularly scans shared files against the **IWF hash list**, automatically blocking any matches. This method is highly accurate and accounts for the vast majority of proactive removals.

In addition, for users in the European Union, PikPak operates an image recognition system that extracts still frames from video files whenever a share link is created or accessed. This measure is implemented in line with **applicable European regulations** ^{[1][2][3]} that permit online service providers to take voluntary measures to detect and address CSAM. Files strongly identified as CSAM are blocked immediately. Where the system produces uncertain matches, the files are referred to a human review team for confirmation. To further ensure accuracy, the review team also conducts **regular checks of machine decisions** to reduce false positives and continuously improve the performance of the image recognition system.

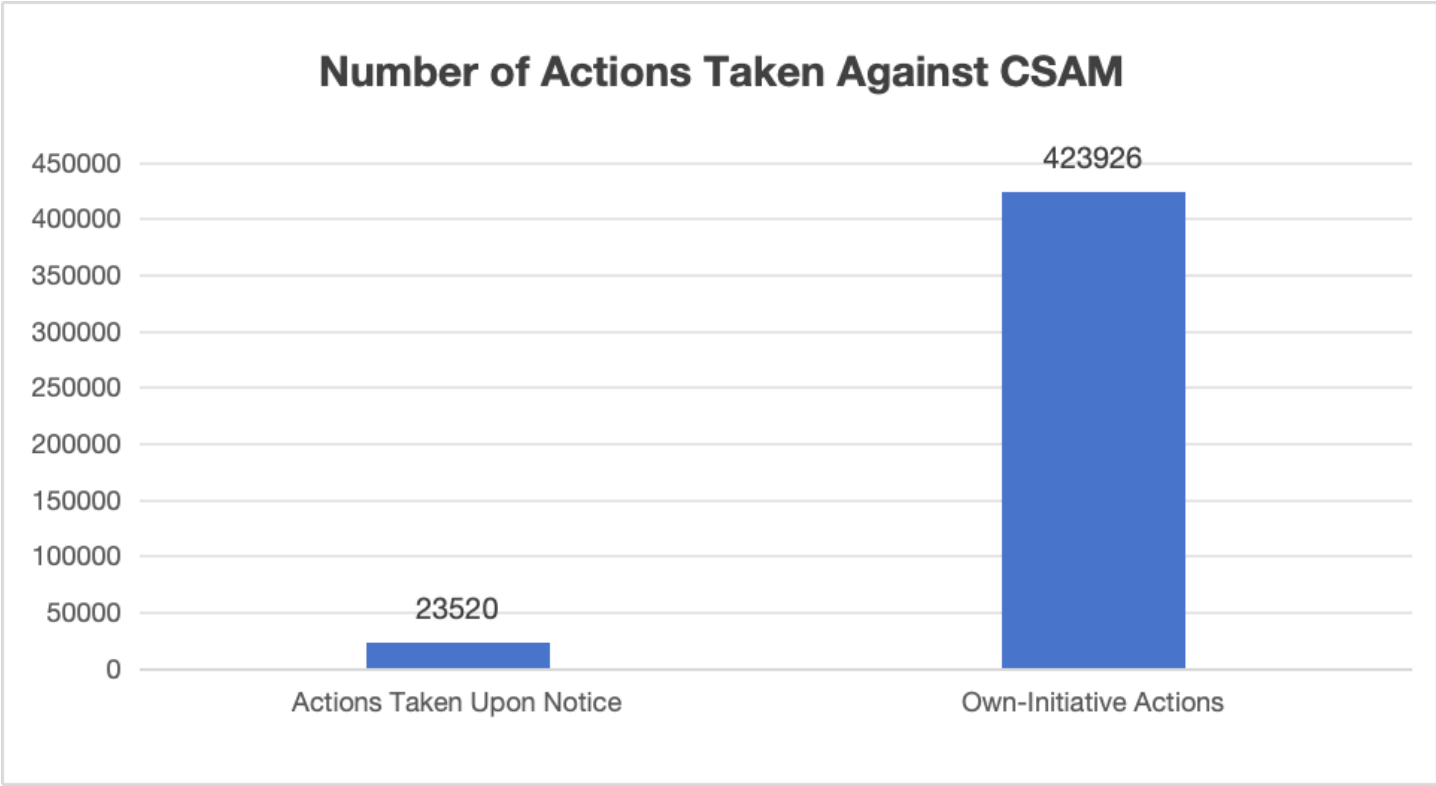


Figure 2 - the vast majority of actions were taken proactively, demonstrating our strong focus on detecting and removing such material before it is reported.

CSAM Links Blocked Through Proactive Detection

■ Image Recognition System ■ IWF Hash-Matching

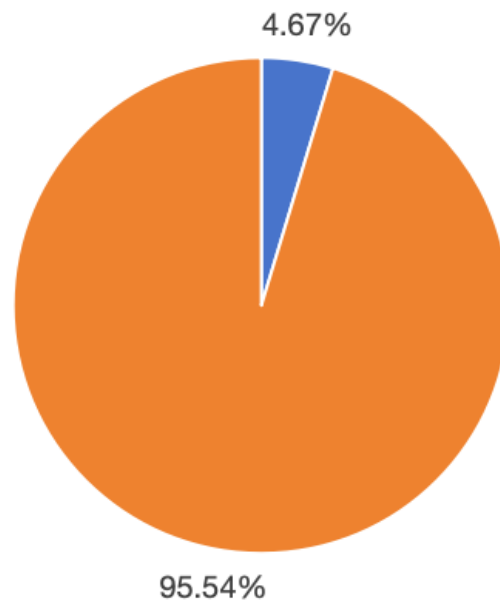


Figure 3 - The vast majority of CSAM links were blocked through IWF hash-matching, while only a small proportion were identified through the image recognition system.

Illegal content may be reported to PikPak by anyone. Reports submitted by organizations such as the IWF, NCMEC, and FSM are treated as **trusted flagger reports**, which we regard as highly reliable. Upon receipt, the reported links are promptly disabled and the associated accounts are closed. The vast majority of reports—approximately **99%**—come from private individuals who encounter links being openly shared on public forums, while only about **1%** originate from trusted flaggers. These reports typically include a description of the content, and since anyone with both the link and the password can access the files, swift action is critical.

Content that requires manual review comes from two primary sources:

1. **Proactive detection** – uncertain cases flagged by the image recognition system.
2. **Reports** – all user reports undergo human assessment.

This review process ensures that questionable or reported content is properly verified before enforcement action is taken.

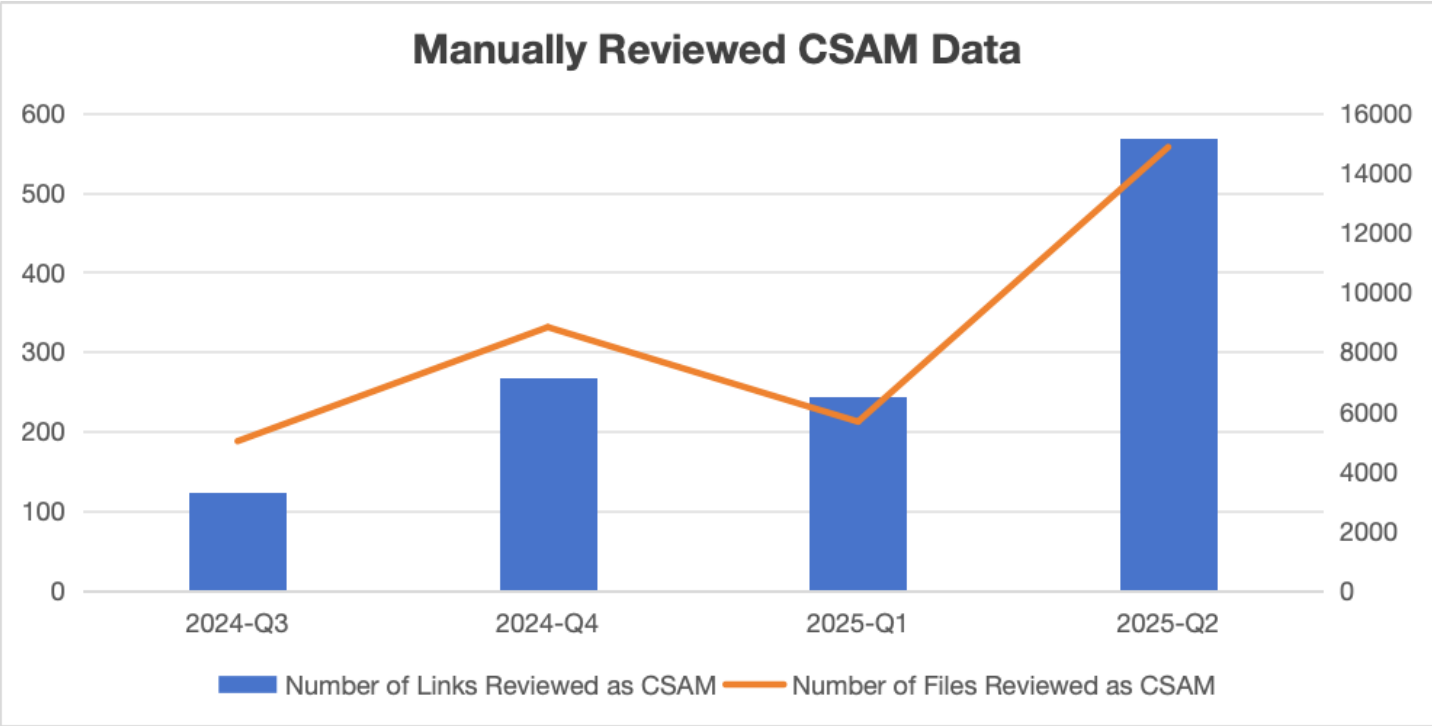


Figure 4 - Manually Reviewed CSAM Data. Typically, a single sharing link may contain multiple files, so the number of files reviewed as CSAM is higher than the number of links.

9. Legal Orders

During the year ended 30 June 2025, PikPak received two orders from agencies regarding alleged CSAM cases.

Originating Country	Alleged Criminality	Number of Orders/Warrants	Outcome
Denmark	CSAM	1	Assistance with faster access to evidence stored in perpetrator's PikPak account
Singapore	CSAM	1	Metadata Supplied

Table 2 - Legal Orders

Under Singapore law, if foreign law enforcement agencies require user registration information, verification details, IP information, or similar data, they must contact the relevant Singapore regulatory authority. That authority can assist in submitting the request to us in accordance with Singapore legal requirements.

Nevertheless, in cases involving serious criminality, PikPak may cooperate in other ways, such as expediting evidence downloads, removing alleged unlawful files, disabling or deleting user accounts, and preserving relevant content when required.

10. Definition of Terms

PikPak uses the term Child Sexual Abuse Material (**CSAM**) to refer to photos, videos, documents, or other files depicting sexually explicit images of, or sexual conduct involving, a child. This definition is consistent with the ECPAT 2016 Luxembourg Guidelines, and broadly aligns with terms used by other platforms, such as Child Sexual Exploitation and Abuse (**CSEA**) and Child Sexual Exploitation and Abuse Imagery (**CSEAI**).

Trusted flaggers are specialized organizations whose reports are considered highly reliable. These include, but are not limited to, the Internet Watch Foundation (**IWF**), the National Center for Missing and Exploited Children (**NCMEC**), and **FSM**.

Suspension refers to the permanent closure of a user account, unless reinstated following a successful appeal. Suspended accounts lose access to all PikPak services, and any content associated with the account is rendered inaccessible.

References

- [1] EU Digital Services Act (DSA) https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en
- [2] CSAR (Child Sexual Abuse Regulation) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0209>
- [3] Temporary Derogation Regulation (Regulation (EU) 2021/1232) <https://eur-lex.europa.eu/eli/reg/2021/1232/oj/eng>