OFCOM FILE SCANNING

Duties for file servers and sharing services

October 2025

Deadline Monday 20 October 2025 and details of how to respond are set out in Annex 1-5.
If you have any questions on the consultation process, please contact us at ASMconsultation@ofcom.org.uk.

Consultation page

PDF document

Action needed:
Email ASMconsultation@ofcom.org.uk and ask for an extension to respond.

Proposals: content scanning duties

ICU C11: Providers should assess whether proactive technology to detect or support the detection of target illegal content is available, is technically feasible to deploy on their service, and meets the proactive technology criteria. If so, they should deploy it.

ICU C12: Providers should assess existing proactive technology that they are using to detect or support the detection of target illegal content against the proactive technology criteria and, if necessary, take steps to ensure the criteria are met.

PCU C10: Providers should assess existing proactive technology that they are using to detect or support the detection of target content harmful to children against the proactive technology criteria and, if necessary, take steps to ensure the criteria are met.

Intimate image abuse (IIA) hash matching ICU C14: Providers use perceptual hash matching to detect image-based intimate image abuse content so it can be removed

Implication

Will impact file-storage and file-sharing services. All will be required to complete a risk assessment and if high risk of image based CSAM.

Further details

Page 77 PDF document

How file sharing services are implicated

Providers of services that are likely to be accessed by children that are:
• large user-to-user services that are medium or high risk for at least one relevant harm
• user-to-user services with more than 700,000 monthly UK users that are high risk, for at least one relevant harm
• user-to-user services that are **file-storage and file-sharing services which identify a high risk of image-based CSAM, regardless of size**
• All user-to-user services which identify a high risk of grooming

Proposal: terrorist scanning

Who should implement this Relevant Code(s) Terrorism hash matching
ICU C13: Providers use perceptual hash matching to detect terrorism content so that it can be removed.

Scope
Impacts large services at medium or high risk or **any file-storage or sharing service at high risk**.

Further details

Page 148 PDF document

Proposal: intimate image abuse scanning

Intimate image abuse (IIA) hash matching
ICU C14: Providers use perceptual hash matching to detect image-based intimate image abuse content so it can be removed

Scope
Will impact all file-sharing and file-storage. Issue is the intimate image abuse database does not verify images creating high risk of system being abused.

More information / questions

Page 128 PDF document