Reference: 2052912

Information Requests

information.requests@ofcom.org.uk

26 August 2025

Freedom of Information request: Right to know request

Thank you for your request for information about data analytics and data sharing under the Online Safety Act 2023.

We received this request on 28 July 2025 and we have considered your request under the Freedom of Information Act 2000 ("the FOI Act").

Your request and our response

Under the Freedom of Information Act 2000, I am writing to request information relating to the data analytics processes and data sharing practices associated with the Online Safety Act 2023, as managed by Ofcom.

I am seeking a clear and comprehensive overview of the following:

1. Data Analytics Processes
A description of the data analytics frameworks, tools, or methodologies used by Ofcom to support the implementation, monitoring, or enforcement of the Online Safety Act 2023.
The types of data collected and analysed (e.g. user data, platform compliance data, or other relevant metrics) to assess compliance with and the overall effectiveness of the Act. Any internal or external reports, policies, or guidance documents outlining how data analytics are applied in relation to the Act.

Given the breadth of the Online Safety Act ("the Act"), Ofcom uses several data analytics frameworks, tools and methodologies to support its activities. For example, standard IT infrastructure and tools for daily use such as MS Suite products, Python, and SQL. In developing our codes of practice we conducted impact assessments of our policy options using information from our consultation responses, quality-assured evidence from academia, civil society, industry and government, and our own programmes of research. Similarly, our monitoring and enforcement work include a range of tools to analyse a diverse set of information, including data we gather directly from service providers, third parties and our own research.

The Act gives us powers to require and obtain information we need for the purposes of exercising, or deciding whether to exercise, our online safety duties and functions. We have issued guidance to help regulated services and other stakeholders understand when and how we might use these powers. Whilst this does not include specific guidance on our use of data analytics, the guidance covers matters such as record retention and personal data, confidential information and disclosure of information, which may be helpful to you.

Our recent transparency statement and final transparency reporting guidance sets out how we will convert data from providers of certain regulated services (specifically those that appear on a public register of "categorised services" prepared by Ofcom) into accessible insights for users. Again, this does not specifically outline how data analytics will be applied, but may provide some helpful detail, including the kinds of information which may be required in Annex 1 of the Final Transparency Guidance. We will prioritise information that helps shine a light on safety risks, measures and governance practices across services.

We have set out our priority areas for research in our online safety research agenda, and we publish the research we conduct on the Ofcom website. We use various research methodologies across many different sources of data including online services data, third-party data feeds and our own consumer research.

We also published a discussion paper in May 2024 which set out how a widely used evaluation framework could be applied to assess the impact and effectiveness of online safety measures. This paper was designed to generate a discussion on the frameworks for evaluating online safety measures amongst services, academics, civil society organisations and the broader trust and safety and online safety expert community.

2. Data Sharing Practices
A list of organisations (such as government departments, agencies, private companies, or international bodies) with whom Ofcom shares data collected under the Online Safety Act 2023. The purposes for which this data is shared (e.g. enforcement, research, or policy development).
Any data-sharing agreements or protocols in place, including details of the measures used to protect personal or sensitive information.

We work with a variety of organisations, details of which (including Memoranda of Understanding) can be found online. Generally, we do not disclose information we have gathered from stakeholders unless: a) we have consent; b) a court or tribunal requires us to disclose the information in relation to civil or criminal proceedings; or c) there is another legal basis for us disclosing the information, and we consider it is proportionate to disclose the information in the circumstances.

Where we have gathered information relating to a particular business using our information gathering powers under the Act, section 393 of the Communications Act 2003 prohibits the disclosure of that information without the consent of the person carrying on that business, unless this is permitted for specific, defined purposes. One of those purposes is where we consider disclosure necessary for the purpose of facilitating the exercise of our online safety functions, or when we are publishing a report under the Act. In these circumstances, we must consider the need to exclude confidential information from publication, so far as practicable.

It is a criminal offence for a person to disclose information in contravention of section 393.

Most of our publications are also shared 24 hours ahead of publication with the UK Government under a pre-disclosure agreement, as required by section 24A of the Communications Act 2023.

The Communications Act 2003 enables Ofcom to share information with certain UK based organisations and offices. The list of relevant persons can be seen at s393(3) of the Communications Act: Communications Act 2003

The Act also enables Ofcom to co-operate with certain overseas regulators listed in regulations made by the Secretary of State, including by disclosing 'online safety information', for certain purposes. The overseas regulators we can disclose information to are:

- l'Autorité de régulation de la communication audiovisuelle et numérique (established in France);
- de Autoriteit Consument & Markt (established in the Netherlands);
- die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (established in Germany);
- Coimisiún na Meán (established in Ireland);
- the eSafety Commissioner (established in Australia);
- the European Commission.

Where Ofcom discloses information to an overseas regulator, that regulator cannot use the information for a purpose other than the purpose for which it was disclosed, or further disclose the information without our consent or by an order of a court or tribunal. We are also prevented from disclosing information to an overseas regulator that would contravene data protection legislation.

All of our work is subject to rules around records management and data protection. More information can be found the online safety information gathering guidance, as well as our broader corporate policies on handling personal data and records and information management.

Ofcom is also a producer of official statistics and follows the principles set out in the Office for Statistics Regulation Code of Practice for Statistics to ensure we produce trustworthy statistics based on data sources of appropriate quality.

3. Third-Party Involvement
Information about any third-party organisations (such as contractors, technology providers, or research institutions) involved in data analytics or data processing in connection with the Online Safety Act 2023.
An explanation of how Ofcom ensures compliance with the UK General Data Protection Regulation (UK GDPR) when sharing data with these third parties.

We often rely on various third-party organisations and/or suppliers to deliver important services that help us to meet our core objectives, including our online safety work. We use a variety of internal tools and applications that include data analytics capability.

We expect any organisations we work with to understand and comply with all legislation relevant to their business and ours, including data protection regulation. This is covered by our Standard Terms and Conditions of Contract for goods or services, details of which are available on our website page providing information about Ofcom's approach to procurement.

Our programme of consumer research is conducted by third-party market research agencies on behalf of Ofcom through competitive tender and follows the Market Research Society Code of Conduct. The agencies we work with can be found in our market research framework. We carry out Data Protection Impact Assessments before undertaking any research to ensure that personal data will be handled appropriately.

We hope this information is helpful. If you have any further queries, then please send them to information.requests@ofcom.org.uk, quoting the reference number above in any future communications.

Yours sincerely

Information Requests

Request an internal review

If you are unhappy with the response you have received to your request for information, or think that your request was refused without a reason valid under the law, you may ask for an internal review. If you do, it will be subject to an independent review within Ofcom. We will either uphold the original decision, or reverse or modify it.

If you would like to ask us to carry out an internal review, you should get in touch within two months of the date of this letter. There is no statutory deadline for us to complete our internal review, and the time it takes will depend on the complexity of the request. But we will try to complete the review within 20 working days (or no more than 40 working days in exceptional cases) and keep you informed of our progress. Please email the Information Requests team (information.requests@ofcom.org.uk) to request an internal review.

Taking it further

If you are unhappy with the outcome of our internal review, then you have the right to complain to the Information Commissioner's Office.