CONFIDENTIAL

Ofcom
Email:
riskassessmentprogramme@ofcom.org.uk

4chan community support LLC

14 April 2025

Our Ref: 01979686

By email

cc. [redacted]

Dear Sir / Madam,

Risk Assessment Enforcement Programme: Notice for information under the Online Safety Act 2023

You will be aware from our letter dated 27 March 2025 that we have launched an enforcement programme to monitor whether providers of regulated services across the sector have complied with their duty to complete, and keep a record of, an **illegal content risk assessment**, in accordance with the Online Safety Act 2023 (the "**Act**").

As part of this programme, we are requiring a number of service **providers**, including 4chan community support LLC, to send us a copy of the **record of the illegal content risk assessment** relating to the service(s) they provide.

Amongst other things, the records provided will help us assess the extent of any compliance concerns and consider an appropriate and proportionate response. We will provide updates on the progress of this programme as it proceeds.

The records of risk assessments will inform our on-going supervisory and compliance activities. They may also inform or be used in relation to internal policy development work relating to our codes of practices or the design of our transparency notices. This request is part of broader efforts by **Ofcom** to understand compliance with relevant duties in the **Act**. We may in due course request your record of the measures (or alternative measures) taken to comply with the safety duties.

I attach a formal request ('Notice') for information under Section 100 of the **Act** addressed to 4chan community support LLC. The Notice includes further details on the background to this information request, and Annex 1 to the Notice sets out the information we require from you.

The deadline for providing the information is **11:00 GMT** on **29 April 2025**.

If you have any queries in relation to this Notice, please email riskassessmentprogramme@ofcom.org.uk. Please quote our reference at the top of this letter.

Yours faithfully,

Ofcom

CONFIDENTIAL

Ofcom

Company Secretary
4chan community support LLC

14 April 2025

Our Ref: 01979686

By email only

cc. advertise@4chan.org; press@4chan.org; bizdev@4chan.org;

Dear Sir / Madam,

Risk Assessment Enforcement Programme: Notice requiring the provision of specified information under Section 100 of the Online Safety Act 2023

This is a formal request ('Notice') for information under Section 100 of the Online Safety Act (the '**Act**') addressed to '4chan community support LLC' ('4chan'), in respect of the service, 4chan.

This Notice requires you to provide the information requested in Annex 1 in the manner and form specified. Further details are set out within the section titled 'When and how must I send the required information?' below.

Background to the request

The **Act** imposes duties on a range of online service providers to keep people who use their service safe from illegal content. Certain duties under the **Act** are now in effect. These duties cover both user-to-user ('U2U') as well as search services, and also apply to individuals who run an online service. It does not matter where a **provider** or their business is based. The new duties apply to **providers** or their business if the service they provide has a significant number of users in the UK, or if the UK is a target market.

Providers of a U2U or search service (or a service that is a combination of these two types of service, a '**combined service**') must carry out an **illegal content risk assessment** of that service. This is a legal obligation under Section 9 of the **Act**, which requires **providers** to assess the risks of their service associated with priority offences and other illegal content.

Providers must also make and keep a written record, in an easily understandable form, of all aspects of every **illegal content risk assessment**, including details about how the assessment was carried out and its findings. This is a legal obligation under Section 23 of the **Act**.

On 16 December 2024, **Ofcom** published Risk Assessment Guidance and Risk Profiles to help **providers** comply with the **illegal content risk assessment** duties. This guidance sets out a four-step risk assessment process, which, if followed, will help **providers** comply with the **illegal content risk assessment** duties. We also published Record-Keeping and Review Guidance to assist **providers** in meeting their duties of keeping records of, and reviewing, their risk assessments.

Following the **illegal content risk assessment** duties and record-keeping duties coming into force, we have launched an enforcement programme to monitor compliance with these duties across the sector. As part of this programme, we have decided to request records of the **illegal content risk**

Ofcom, Riverside House, 2a Southwark Bridge Road, London SE1 9HA
Switchboard: 0300 123 3000 or 020 7981 3000
www.ofcom.org.uk

assessments from a range of providers of in-scope services Ofcom considers may present particular risks of harm to UK users from illegal content due to their size and/or nature.

We will use the information provided in relation to our enforcement programme, including to assess your compliance with your duties. Records of risk assessments may also inform, or be used, in relation to our supervisory activities, internal policy development work relating to our codes of practices or the design of our transparency notices.

Why have I been sent this Notice?

We are sending this Notice to you because **Ofcom** considers that:

(a) you are a provider of a U2U service[1]; and/or

(b) you hold, or are able to generate or obtain, information which is relevant for assessing your compliance with both the record-keeping duties and the illegal content risk assessment duties.

We have selected your service because Ofcom considers that the size and/or nature of your service is such that it may present particular risks of harm to UK users from illegal content.

The **illegal content risk assessment** duties came into force on 16 December 2024, and you had until 16 March 2025 to complete your first **illegal content risk assessment** of the above service. You must make and keep a written record of your risk assessment in accordance with the record-keeping duties.[2] Please consult our Record Keeping and Review Guidance to ensure your record provides all necessary details, including the role of any existing controls already in operation on the service at the time of the risk assessment.

As explained above, the purpose of sending you this Notice is to gather information that is relevant to our enforcement programme, which may include consideration of your compliance with these duties, as a provider of an in-scope service. Annex 1 to this Notice requests that you provide a copy of your record of the **illegal content risk assessment** in respect of the service you provide. As we are requiring the provision of a record that you must produce to comply with your duties under the Act, we consider that responding to the request will not impose a significant burden and that the request is therefore proportionate.

Final Information Notice

It should be noted that **Ofcom** would normally send a draft version of an information request to the recipient, providing the opportunity for comments on the draft. This would be followed by the final information request. However, in this specific case we have exercised our discretion not to send a draft information request given the straightforward nature of the request, the fact that we are

[1] Please refer to Section 100(5)(a) and (f) of the Act.
[2] Record-keeping and review duties as set out in Section 23 of the **Act**.

requesting information which you should already hold and the fact that you have been advise that the request was coming. This is in line with our Online Safety Information Gathering Guidance.

What must I do now?

Annex 3 to this Notice sets out detailed information on what you need to do to comply with this request. In particular, you must:

- Answer the question in Annex 1 and ensure your response is complete, fully accurate, and up-to-date;
- Provide the information requested in the manner and form specified in this Notice and its Annexes;
- Provide all the information we have asked for even if it is commercially sensitive, contains personal data or you believe it may harm your reputation; and
- Provide your response no later than **11:00 GMT** on **29 April 2025** ('the deadline')**.**

If you do not comply with the above, we may decide to take enforcement action and you may receive a significant financial penalty. A failure to comply with a requirement of an information notice may also constitute a criminal offence. Further information on the consequences of failing to comply with this Notice is set out in Annex 3 below. Given the seriousness of the potential consequences, you may want to seek your own independent legal advice about this request.

Structure of request

This Notice has the following Annexes:

Annex 1: *Information required under Section 100 of the Act* - This sets out all the questions you need to answer.

Annex 2: *Key definitions* - This contains a table setting out definitions of the terms used within this Notice.

Annex 3: *More information* – This sets out the following questions and answers you may have about this Notice or your response:

What do I need to do now?

How should I provide the information to Ofcom?

What if I cannot meet the deadline?

How do I answer the request on behalf of a corporate group?

What happens if I do not have the information requested?

What do I do if there is confidential information included in my response?

How does Ofcom treat confidential information?

How does Ofcom treat personal data?

Enforcement and offences – what happens if I fail to respond to this Notice?

Annex 4: *Managed File Transfer information sheet* – This sets out information about Ofcom's Managed File Transfer system.

If you have any queries about this Notice, please email riskassessmentprogramme@ofcom.org.uk. Please quote our reference at the top of this letter.

Should you be unable to meet the deadline for responding to this Notice, please contact riskassessmentprogramme@ofcom.org.uk urgently, and in any event before the deadline has passed. Please explain why the deadline cannot be met.

Yours faithfully,

Ofcom

Enc:
Annex 1: Information required under Section 100 of the Act
Annex 2: Key definitions
Annex 3: More information
Annex 4: Managed File Transfer information sheet

Annex 1: Information required under Section 100 of the Act

You must provide a complete and accurate response to the question set out below. Please refer to Annex 3 for more information that may assist you in understanding how to respond to this notice.

Record of illegal content risk assessment

In accordance with Section 23 of the **Act**, all **providers** of U2U services must make and keep a written record of all aspects of every **illegal content risk assessment**, covering the required elements in Section 9 of the **Act**.

1. Please provide us with a copy of the written record of your illegal content risk assessment in respect of 4chan.

Annex 2: Key definitions

In this Notice, except insofar as the context otherwise requires, words or expressions shall have the meaning assigned to them in the table below.

Term	Meaning
Act	The Online Safety Act 2023
Combined service	A **regulated user-to-user service** that includes a public search engine.[3]
Illegal content risk assessment	Risk assessments carried out under Section 9 of the Act.
Ofcom	The Office of Communications, known as Ofcom, is the UK's independent regulator for online safety under the **Act**. Ofcom has statutory responsibilities under the **Act** to regulate certain internet services. For more information about **Ofcom**, see: https://www.ofcom.org.uk/about-ofcom/what-is-ofcom.
Provider of a regulated service[4] (also referred to as 'provider')	The **provider** of a **regulated service** is the entity, and that entity alone, who: • for **regulated user-to-user services**, has control over who can use the user-to-user part of the service; or • for **regulated search services**, has control over the operations of the search engine. Where no such entity exists, the **provider** will be the individual or individuals with this control.
Record of the illegal content risk assessment	A written record, in an easily understandable form, of all aspects of every risk assessment under Section 9, including details about how the assessment was carried out and its findings.
Regulated service[5]	Any of: • a **regulated user-to-user service**,[6] or • a **regulated search service**.[7]

[3] Section 4(7) of the **Act**.
[4] Section 226 of the **Act**.
[5] Section 4(4) of the **Act**.
[6] '**user-to-user service**' means an **internet service** by means of which content that is generated directly on the service by a **user** of the service, or uploaded to or shared on the service by a **user** of the service, may be encountered by another **user**, or other **users**, of the service. See Section 3(1) of the **Act**.
[7] '**search service**' means an **internet service** that is, or includes, a search engine. See Section 3(4) of the **Act**.

Term	Meaning
	Services will be regulated if they have links with the UK,[8] and are not exempt.[9]

[8] A **user-to-user or search service** will have **links with the UK** if:

- it has a significant number of **users** in the UK;
- the UK is a target market; or
- it is capable of being used by individuals in the UK and there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the UK because of the user-generated content present on the service or search content (as relevant). See Sections 4(5) and (6) of the **Act**.

A **Part 5 online pornography service** has **links with the UK** if:

- it has a significant number of **users**; or
- UK **users** form one of the target markets. See Section 80(4) of the **Act**.

[9] For **exempt user-to-user and search services**, see Schedule 1 of the **Act**. **Regulated user-to-user** and **search services** do not include a service combining user-generated content or search content not regulated by the **Act** with **pornographic content** that is regulated (Section 4 of the **Act**).
For **exempt Part 5 online pornography services**, see Schedule 9 to the **Act**.

Annex 3: More information

This Annex sets out more information about this request and how to respond to this Notice.

What do I need to do now?

You must provide or, if necessary, obtain or generate all the information we have requested under this Notice. The information you provide in response to this Notice must be complete, fully accurate and up-to-date. This means you must provide all the information we have asked for even if it is commercially sensitive, contains personal data or you believe it may harm your reputation. There may be legal repercussions if you fail to provide a full, accurate and timely response to our questions (see below).

How should I provide the information to Ofcom?

You must provide the information we have requested no later than the deadline in the Notice.

You should provide the information electronically, preferably via our secure Managed File Transfer (MFT) system or alternatively by email to riskassessmentprogramme@ofcom.org.uk.

If you wish to use the MFT system, please email riskassessmentprogramme@ofcom.org.uk, at least three working days before the deadline, providing the name and email address of your nominated contact who will upload the data, so that we can set up an account. An information sheet about the MFT system is attached to the Notice at Annex 4.

What if I cannot meet the deadline?

Should you be unable to meet the deadline for responding to this request, please contact riskassessmentprogramme@ofcom.org.uk urgently, and in any event before the deadline has passed. Please also explain why the deadline cannot be met.

We only agree to extend deadlines where there are good reasons for doing so, like:

- unexpected absence of a key employee responsible for obtaining the required information;
- technical difficulties; or
- other exceptional circumstances outside of your control.

Every extension request will be considered on its own merits.

How do I answer this request on behalf of a corporate group?

You are legally required to provide the information requested, including by obtaining or generating information which relates to or is held by your Subsidiary[10] or Subsidiaries unless there are specific reasons why it is not possible to provide the requested information. If that is the case, you must make this clear in your response.

[10] A **Subsidiary** is a business entity, company or corporation which is owned or controlled (directly or indirectly) by the person to whom this Notice is addressed. For these purposes, this means the person to whom this Notice is addressed (or an entity/company/corporation owned or controlled by that person) owns the majority of the share capital and/or exercises the majority of the voting rights or is otherwise able to exercise dominant influence over it (e.g. due to contractual arrangements or as set out in the entity/company/corporation's constitution).

It is important to note that as the named recipient of the Notice you are the person legally responsible for complying with it, including ensuring that the information is fully accurate and complete, and provided in the manner and form requested, by the date specified in the Notice.

What happens if I do not have the information requested?

Ofcom can require you to obtain or generate the information requested in this Notice. This means that even if you do not hold the relevant information within your corporate group, you are still required to take certain steps so that it can be provided to us. Therefore, in your response to this Notice, and as applicable, you must take the following steps:[11]

- Where a particular question asks for information that you have or can provide but you do not currently hold it in the manner or form requested, you must generate the information in the manner and form requested if you are able to do so.[12]
- Where a particular question asks for information that is held by, or can be generated or obtained by, your **Subsidiary**, you must obtain that information from the **Subsidiary** unless you are unable to do so.
- If you do not consider you hold or are able to generate or obtain the relevant information, or if you are only able to provide some but not all of the information, or if you are not able to provide the information in the manner and form requested, you must explain why.
- If you are aware of another person who holds or may hold the requested information which you cannot obtain, please provide the name, email address and/or telephone number of that person.

For the avoidance of doubt, we do not require you to obtain information that you don't already hold from third parties (i.e. persons that are not your **Subsidiaries**).

What do I do if there is confidential information included in my response?

You must provide the information requested in this Notice, even if you consider that the information, or any part of it, is confidential. This includes, for example, information that is confidential due to commercial sensitivity or relating to third party confidentiality undertakings.

Ofcom's usual practice is to ask respondents to information notices to confirm, in response to the Notice, if any of the information they are required to provide under the notice is confidential and to provide a written explanation as to why the information should be treated as confidential. We are **not** asking for you to do this for the purposes of your response to this particular Notice, as it is not Ofcom's intention to publish your response to the Notice. However, as explained in more detail below, if we later propose to disclose any of the information you have provided, we will normally seek your representations on that disclosure in the first instance.

Ofcom will take into account any claims that information should be considered confidential. However, it is for **Ofcom** to decide what is or is not confidential, taking into account any relevant common law and statutory definitions. We do not accept unjustified or unsubstantiated claims of confidentiality. Blanket claims of confidentiality covering entire documents or types of information are also unhelpful and will rarely be accepted. For example, we would expect stakeholders to

[11] Section 100(2) of the **Act**.
[12] This could mean, for example, undertaking calculations, data extractions or another methodology to work out performance metrics or re-producing and combining data from different sources.

consider whether the fact of the document's existence or particular elements of the document (e.g. its title or metadata such as to/from/date/subject or other specific content) are not confidential.

Any confidential information provided to **Ofcom** is subject to restrictions on its further disclosure as explained further below. For this reason, we do not generally consider it necessary to sign non-disclosure agreements. Our general approach to the disclosure of information is set out below.

For the avoidance of doubt, stakeholders are not required to provide information that is legally privileged and can redact specific parts of documents that are legally privileged. Please note that just because an email is sent to or from a legal adviser does not mean it is necessarily a legally privileged communication. Further information is available in our Online Safety Information Gathering Guidance.

Will Ofcom disclose any of my response?

Circumstances in which we may disclose information that we have gathered

General

We will not disclose information we have gathered from stakeholders unless:

a) we have consent;
b) we are required by a Court or Tribunal 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, section 393 of the Communications Act 2003 explains that **Ofcom** cannot disclose that information without the consent of the person carrying on that business, unless this is permitted for specific, defined purposes (and in many cases only to specific persons), as set out in sub-sections (2) to (7). One of those purposes is where we consider disclosure necessary for the purpose of facilitating the exercise of our online safety functions. It is a criminal offence for a person to disclose information in contravention of section 393.

The general restriction under section 393 of the Communications Act does not apply in certain circumstances, namely:

a) where **Ofcom** is publishing a report under the **Act** or is arranging for the publication of its advice to the Secretary of State as to the categorisation of regulated user-to-user services and regulated search services. In these circumstances, **Ofcom** must have regard to the need to exclude from publication, so far as practicable, confidential information.[13]
b) when **Ofcom** is publishing details of enforcement action under the **Act**. In this circumstance, **Ofcom** may not publish confidential information.[14]

Ofcom will generally redact information identified as confidential from our publications or withhold it from the disclosures we make. However, for the avoidance of doubt, we may disclose such

[13] In the case of a report, see Section 393(6)(b) of the Communications Act and Section 164 of the **Act**. In the case of Ofcom's advice, see Section 393(6)(a) of the Communications Act and Schedule 11, paragraph 4, to the **Act**.
[14] See Section 393(6)(a) of the Communications Act and Section 149 of the **Act.**

information where permitted by law. For example, **Ofcom** may disclose information to facilitate the carrying out of our functions by ensuring stakeholders can properly understand the basis for our reasoning.[15]

In some cases, we may decide not to publish certain information, even where it is not confidential. For example, we may decide not to publish distressing material such as narratives about suicide, on the basis that this could cause undue distress and would not facilitate the exercise of our functions.

Disclosure to overseas regulators

The Act also enables **Ofcom** to co-operate with an overseas regulator listed in regulations made by the Secretary of State, including by disclosing 'online safety information',[16] for certain purposes. Those purposes are:

a) to facilitate the online safety functions of the overseas regulator which correspond to **Ofcom's** functions under the **Act** (the 'online regulatory functions'); or
b) criminal investigations or proceedings relating to a matter to which the overseas regulator's online regulatory functions relate.[17]

Only the Secretary of State can decide which overseas regulators **Ofcom** has the power to disclose information to under this mechanism.[18]

The Secretary of State may update this list over time.

The **Act** puts in place various safeguards concerning the overseas regulator's treatment of the information that **Ofcom** discloses. Where **Ofcom** discloses information to an overseas regulator, they may not:

a) use the information for a purpose other than the purpose for which it was disclosed; or
b) further disclose the information;

without **Ofcom's** consent or in accordance with an order of a court or tribunal.[19]

The **Act** also puts in place various limitations on **Ofcom's** power to disclose information to an overseas regulator, including that **Ofcom** may not make a disclosure that would contravene data protection legislation.[20]

The process we expect to follow if we proposed to disclose information

When deciding whether to disclose information we will carefully balance the need to disclose the relevant information against any concerns or objections raised by the person who provided the information in relation to the disclosure.

We may have explained our intention to disclose the information in any draft or final statutory information notice. If we have not and subsequently propose to disclose information, we will normally first explain our intention to disclose the information (including the context in which we intend to disclose it) and give that person the opportunity to make representations about the

[15] Our regulatory activities should also be transparent and accountable (section 3(3)(a), Communications Act).
[16] 'Online safety information' is defined as information held by Ofcom in connection with any of Ofcom's online safety functions: section 114(7) of the Act.
[17] Section 114(1) of the **Act**.
[18] Section 114(2) of the **Act**, which gives the Secretary of State the power to make secondary legislation setting this out, which must be passed by the UK Parliament.
[19] Section 114(3) of the **Act**.
[20] Section 114(5)(b) of the **Act**.

proposed disclosure. There may be circumstances where this is not appropriate, for example where we are disclosing information to an overseas regulator for the purpose of an overseas criminal investigation relating to the overseas regulator's online regulatory functions and giving notice of our intention to disclose the information to the overseas regulator could prejudice their investigation.

We will generally try and resolve any objections to a proposed disclosure through constructive dialogue. If we remain of the view that we need to disclose the information and the person concerned continues to object, we will give them advance warning prior to make the disclosure. This will give the person concerned an opportunity to challenge our decision to raise the issue with the Procedural Officer, where relevant.[21]

Where **Ofcom** decides the information provided does not need to be disclosed in full but considers it appropriate to include some information in a proposed disclosure, we may ask the person concerned to provide a summary of information or a range of numbers for the purposes of including this in the relevant disclosure, rather than simply removing the information.

Where in order to exercise our functions under the **Act** there is a need to disclose information regularly, a different process for disclosing information may be appropriate. Where we intend to take a different approach to that set out above, we would expect to explain our approach to stakeholders in advance of disclosing any information.

Our Online Safety Enforcement Guidance provides further information about our approach to disclosing confidential information during an investigation. This would apply to information we have obtained for the purposes of an investigation using our information gathering powers.

Freedom of information requests

As a public authority, **Ofcom** is subject to the Freedom of Information Act 2000 (the 'FOI Act') meaning it has a general duty to provide access to information that is requested by a third party. However, a number of exemptions may apply in which case **Ofcom** is not required to disclose the requested information.[22] The applicability of any exemption will depend on the nature of the information sought by any FOI request made.

In particular, Section 44 of the FOI Act exempts information from disclosure if its disclosure is prohibited under another enactment.[23] This means that where we have gathered information relating to a particular business (either using our information gathering powers under the **Act** or on a voluntary basis), we are prohibited from disclosing that information in response to a FOI request, unless we have the consent of that business.

If we decide that we cannot disclose information because an FOI exemption applies, it is unlikely to be necessary to discuss this with the business that provided the information to us.

If we need more information to help us determine whether an FOI exemption applies, we will discuss the request with the business that provided the information to us. We are subject to statutory deadlines for responding to FOI requests and expect a prompt reply.

[21] Section 10 of our Online Safety Enforcement Guidance explains when a procedural complaint can be referred to Ofcom's Procedural Officer and the process for doing so.
[22] The Information Commissioner's Office provides guidance on the exemptions that may apply.
[23] For example, where disclosure is prohibited under section 393 of the Communications Act.

How long will Ofcom retain my response for and how does Ofcom treat personal data?

As a public authority, we will need to retain information as part of the evidence base underlying any decision we reach. We will keep information in line with our records and information management policy.

We may use this request to obtain personal data if we consider that this information is necessary and relevant for the purpose of our functions. Personal data is defined in Article 4 of the UK General Data Protection Regulation ('GDPR') as information relating to an identified or identifiable person[24].

In general, our role under the **Act** focuses on tackling the root causes of online content that is illegal or harmful to children, by improving the systems and process that services use to address them. Consistent with that role, in many cases it will not be necessary to use our statutory information gathering powers to obtain personal data to enable us to perform our online safety functions. However, there may be circumstances where obtaining personal data is necessary. For example, where we obtain emails or meeting minutes from a service provider, this may include the names or email addresses of individuals employed by that provider, where these are relevant.

In all cases, **Ofcom** will seek to limit the personal data which it requires under its information gathering powers to that which is necessary for the performance of our functions under the **Act**.

Those subject to our information gathering powers will be responsible for complying with their own obligations under relevant data protection legislation. Any personal data they process in responding to our request for information is processed by them on their own account, as a data controller, rather than as a processor of that data for **Ofcom**. Our information gathering powers are not capable of requiring a person to process personal data in a way that contravenes UK data protection legislation,[25] including the UK GDPR. However, in determining whether the processing of personal data would contravene UK data protection legislation, the duty to provide the requested information should be taken into account.[26] Under Article 14 of the UK GDPR, where we (as data controller) have obtained personal data other than from the data subject, we must provide the data subject with certain information.[27] However, there are various exceptions to this obligation, which we will consider on a case-by-case basis. These exceptions include where providing the data subject with the required information would seriously impair our ability to achieve the objectives of the processing, or would involve a disproportionate effort,[28] taking account of any measures to protect the data subject's rights, freedoms and legitimate interests.[29] In making that assessment we would

[24] An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person: see Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation).

[25] UK data protection legislation means the legislation identified in section 3(9) of the Data Protection Act 2018.

[26] Under the UK GDPR, a person has a lawful basis for processing personal data if that is necessary for compliance with a legal obligation to which the controller is subject: Article 6(1)(c).

[27] UK GDPR, Article 14(1)-(3).

[28] UK GPDR, Article 14(5).

[29] When relying on the 'disproportionate effort' exception, it is necessary to assess whether there is a proportionate balance between the effort involved in providing the data subject with the required information and the effect that the use of their personal data will have on them. See ICO: Are there any exceptions? | ICO.

take into account that we would not expect to disclose any personal data unless we are satisfied that it is necessary to do so and that we have a legal basis to do so under data protection law.

Ofcom's General Privacy Statement contains further information about how **Ofcom** will handle personal data.[30]

Enforcement and offences – what happens if I fail to respond to this Notice?

You have a legal duty to comply with this Notice under Section 100 of the **Act**. This means that you must act in accordance with this Notice, providing all the specified information by the applicable deadline.[31] You must also ensure that the information provided in it is complete and accurate in all material respects.[32]

Failure to comply with this Notice may result in **Ofcom** taking enforcement action against you, such as requiring you to take certain steps to comply[33] and/or imposing a financial penalty.[34] The financial penalty could be up to whichever is greater of £18 million or, in certain circumstances,[35] 10% of the person's qualifying worldwide revenue.[36] [37] A daily rate penalty may also be applied in addition to a fixed rate penalty.[38]

If you are the **provider** of a **regulated service** to which this Notice relates, you may be committing an offence under Section 109(1) of the **Act** should you fail to comply with a requirement of the Notice, unless you can show that:

- it was not reasonably practicable to comply with the requirements of the Notice at the time required by the Notice; and
- you have subsequently taken all reasonable steps to comply with those requirements.[39]

The court may require a person convicted of this offence to comply with a requirement of the Notice,[40] or to pay a fine.[41]

Other offences in relation to the Notices include: knowingly providing information that is false in a material respect;[42] providing the information in an encrypted form so that **Ofcom** cannot understand it, with the intention of preventing **Ofcom** from understanding the information;[43] or suppressing, destroying or altering information that is required under the Notice, to prevent **Ofcom** from

---

[30] https://www.ofcom.org.uk/about-ofcom/foi-dp/general-privacy-statement
[31] Section 102(8)(a) of the **Act**.
[32] Section 102(8)(b) of the **Act**.
[33] Sections 130-133 of the **Act**.
[34] Section 137(1) of the **Act**.
[35] Those circumstances are where the penalty is imposed on a person in respect of a **regulated service provided** by that person and qualifying worldwide revenue regulations are in force. **Ofcom** will make regulations determining the qualifying worldwide revenue for the online safety fees regime and for the purposes of considering financial penalties for group entities, see ss 85(1)(a) and (6) and paragraph 5(9), Schedule 13 to the **Act**. Please note that, at the time of this Notice, no such regulations have yet been made.
[36] Paragraphs 4 and 5 (groups of entities), Schedule 13 to the **Act**.
[37] In particularly serious cases, and where applicable, **Ofcom** may take business disruption measures to restrict the service in question. See Sections 144-148 of the **Act**.
[38] Section 137(1)(b) of the **Act.**
[39] Section 109(7) of the **Act**.
[40] Section 109(8) of the **Act**.
[41] See Sections 113(1)(a)-(c) of the **Act**.
[42] Section 109(3) of the **Act**.
[43] Section 109(4) of the **Act**.

obtaining the information or obtaining the information in the unaltered form.[44] A person who is convicted of any of these offences may face imprisonment for a term of up to two years, or a fine (or both).[45]

You are therefore required to ensure that your response is on time, complete and accurate. Given the seriousness of the potential consequences, you may want to seek your own independent legal advice about the contents of this Notice.

For more details on our information gathering powers, please see our our Online Safety Information Gathering Guidance.

[44] Section 109(5) of the **Act**.
[45] See Sections 113(2)(a)-(d) of the **Act**.

Annex 4: Managed File Transfer information sheet

Managed File Transfer

Managed File Transfer (MFT) allows Ofcom to share files with external organisations securely. It provides a full audit trail of activity. There are two methods for sending and receiving files - shared folders and Packages. Your Ofcom contact will arrange the most appropriate one for your purposes.

Packages

For one-off file transfers or occasional use, MFT provides a secure Package facility that works in a similar way to email messaging.

You do not need an account on MFT to access a Package. When someone from Ofcom sends you a package you will receive an email notification from MFT with a link to the Package.

Your Ofcom contact will provide you with a password to access the package. You can then download any attached files.

To send data using this method, someone at Ofcom must first send you a package. You can then reply – attaching any files you want to share with your Ofcom contact.

Shared Folders

For users who need to transfer files to or from Ofcom regularly, MFT provides a secure transit folder facility. Your Ofcom contact will request an MFT account for you. They will be asked to provide your name, email address and company name.

Your username will be **firstname.lastname_company**.

Once your account has been created, your Ofcom contact will notify you of your temporary password separately. You will be required to change this when you first log on to MFT.

After logging on you will be able to navigate to the shared folder to upload or download files as agreed with your Ofcom contact



Security Fact Sheet

- During transport MFT uses TLS to encrypt communications. The minimum strength of the encryption used during web transport is 128-bit and the system is regularly penetration tested.
- MFT stores all files on disk using FIPS 140-2 validated 256-bit AES. Each file has a unique encryption key, which is also encrypted.
- MFT logs all signon and signoff events, permission changes, new user additions and other actions which directly affect the security of the system. All log entries are cryptographically chained together in a way that makes any tampering of audit logs evident.
- MFT uses cryptographic methods to verify files have not been tampered with.
- Please note that MFT is a tool for transferring files only. To prevent data falling fallow, files are automatically deleted after a set period.
- Only encrypted Zip file format (.7z or .zip) files should be uploaded into MFT