The Information Commissioner's response to Ofcom's consultation on protecting children from harms online

About the Information Commissioner

The Information Commissioner has responsibility for promoting and enforcing data protection and information rights. This includes responsibilities under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and the Privacy and Electronic Communications Regulations 2003 (PECR).

The Information Commissioner is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner provides guidance and support to individuals and organisations, aimed at helping organisations to comply, and takes appropriate action where the law is broken. The ICO's strategic objectives include safeguarding and empowering people and empowering responsible innovation.

The protection of children's privacy online is a prime concern for the ICO. In April 2024, the ICO published its priorities for protecting children's privacy for 2024-25. These include default privacy and geolocation settings, the use of children's information in recommender systems, and the use of information of children under 13.

The ICO's Children's code (also known as the Age Appropriate Design Code) is a statutory code of practice for information society services[1] that are likely to be accessed by children. The code contains fifteen standards that information society services that are likely to be accessed by children should conform to, to comply with their data protection obligations to protect children's data online.

In January 2024, the ICO published an updated opinion setting out the Commissioner's expectations for age assurance under the Children's code (the Opinion). The Opinion explains how age assurance can form part of an appropriate and proportionate approach to reducing or eliminating the personal information risks that children face online. It also sets out the ICO's expectations for data protection compliance when age assurance is deployed, including where it is required under the Online Safety Act (OSA).

[1] 'Information society service' is defined as: "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."

Executive Summary

Overview

- Compliance with many of the online safety duties will inevitably involve the processing of personal data. It is essential that users of online services have confidence that their privacy will be protected. We expect services to comply fully with data protection law when meeting their online safety obligations.
- We are pleased that Ofcom has referred to compliance with data protection law throughout the documents under consultation. We share Ofcom's commitment to promoting compliance across both of our regimes.

Age assurance measures

- Deploying measures from Ofcom's list of potentially 'highly effective' age assurance methods does not automatically ensure compliance with data protection laws. Services must still ensure that they satisfy their data protection obligations. Our Commissioner's Opinion on Age Assurance will help them to comply.
- Ofcom should make it clear that its assessment of the accuracy of age assurance technologies to determine the age of a child (other than over and under 18) is solely about whether age assurance solutions satisfy the 'highly effective' criteria that it applies to the online safety regime.
- The fairness criterion for 'highly effective' age assurance outlined in Annex 10 should align with the requirements of fairness under data protection law so that services are clear that the requirements across the regimes are consistent.

Terms of Service and minimum age restrictions

- Ofcom should provide further clarification on the requirement for services to apply their terms of service consistently where they voluntarily set minimum age requirements.

User reporting and complaints

- For user access measures (AA1 and AA2), Ofcom should more clearly signpost data protection requirements for services to implement tools that allow individuals to challenge inaccurate age assurance technologies.
- We also recommend that Ofcom sets out an effective redress mechanism for these specific measures.

ICO and Ofcom collaboration

As the bodies responsible for regulating data protection and online safety in the UK, the ICO and Ofcom share a commitment to protecting people online. We published a joint statement in 2022 which set out our overall vision of ensuring coherence across online safety and data protection requirements and promoting compliance with both regimes. In May 2024, we deepened our collaboration and published a second joint statement explaining how we intend to collaborate on supervision and enforcement on issues that are relevant to both regimes.

Compliance across the data protection and online safety regimes

The ICO welcomes the online safety regime and its objective to make the UK the safest place in the world to be online. We have engaged with Ofcom during the development of some of the documents subject to this consultation, and we welcome the opportunity to respond to the consultation in full. We stand ready to continue our engagement as Ofcom finalises the measures and guidance.

Compliance with many of the online safety duties will inevitably involve the processing of personal data. It is essential that users of online services have confidence that their privacy will be protected. The OSA has been designed to work alongside data protection law, for which the ICO remains the statutory regulator. We expect services to comply fully with data protection law when following the guidance and implementing the measures recommended by Ofcom in this consultation.

Service providers should familiarise themselves with the data protection legislation, the ICO's Children's code (the Children's code) and relevant ICO guidance, including the Opinion, to understand how to comply with the data protection regime. We expect services to take a data protection by design and by default[2] approach[3] when implementing online safety systems and processes. The privacy duties set out at sections 22 and 33 of the OSA confirm the importance of data protection compliance by requiring services to have particular regard to the importance of protecting users from a breach of any statutory provision or rule of law concerning privacy when deciding on and implementing safety measures and policies.

[2] Art. 25 GDPR – Data protection by design and by default - General Data Protection Regulation (GDPR) (gdpr-info.eu)
[3] Data protection by design and default | ICO

Response to consultation recommendations

In this response, when we mention 'harms', unless otherwise stated, we mean harms defined in s234 of the OSA[4]. Where we refer to harms arising from personal data processing, we make this clear.

We have structured our response in the following sections:

- Section 1: This addresses the proposed codes measures and accompanying sections of volume 5 of the consultation documents in which we have a particular regulatory interest. We have included our response to Annex 10 ('highly effective' age assurance guidance) in this section.

- Section 2: This addresses the risk assessment guidance.

- Section 3: This addresses other draft guidance which present potential issues of data protection compliance (the Guidance on Content Harmful to Children and the Child Access Assessment Guidance).

Overall, we are pleased to note that Ofcom has highlighted the need for compliance with data protection law throughout the documents under consultation. We encourage Ofcom to continue to reinforce the importance of data protection compliance and to refer services to relevant ICO guidance resources where appropriate.

Section 1: The draft Protection of Children Codes of Practice and volume 5

Age assurance

Draft guidance on 'highly effective' age assurance (Annex 10)

We have previously responded to Ofcom's consultation on its draft guidance on 'highly effective' age assurance for providers of pornographic services under Part 5 of the OSA. Given the close alignment between the two pieces of guidance, the views expressed in our Part 5 response also apply to this draft guidance and we refer Ofcom to that response.

In the response to this consultation, we highlight the following points:

'Highly effective' age assurance and data protection compliance

[4] Online Safety Act 2023 (legislation.gov.uk)

Ofcom has provided examples of types of age assurance that could be 'highly effective' (depending on how they are deployed)[5].

When services deploy 'highly effective' age assurance they will process personal data. We are pleased that the guidance reminds service providers that they should familiarise themselves with data protection legislation and how to apply it to age assurance methods by consulting our guidance.

Section 6 of the Opinion sets out our expectations for age assurance and data protection compliance, including the need for services to take a data protection by design approach. In essence, this means services have to integrate appropriate technical and organisational measures into the design and implementation of their systems and processes to implement the data protection principles effectively and safeguard individual rights. Services should be in no doubt that this requirement applies where age assurance is deployed to meet the OSA duties.

We wish to stress that implementing a type of age assurance from Ofcom's list of potential 'highly effective' age assurance methods will not guarantee that the processing of personal data will be compliant with data protection law. Services must ensure that the amount of personal information they collect about a person to verify or assure their age is limited to what is necessary[6]. It will also be important that age assurance is not implemented in a disproportionately intrusive manner. Where 'highly effective' but less intrusive methods are available, they should be used.

We suggest that the draft guidance could specifically refer services to section 6 of the Opinion, which sets out the data protection expectations for services using age assurance. Services could also be referred to the importance of data protection by design which is addressed in section 6.1.9 of the Opinion.

Fairness

The criteria for 'highly effective' age assurance include 'fairness'. This is described as the extent to which an age assurance method avoids or minimises unintended bias and discriminatory outcomes (Annex 10 Box A10.15, page 15).

Data protection law has a separate fairness requirement. It also requires that the risk of bias and discrimination must be minimised. However, the concept of fairness under data protection law[7] is broader. It means that a

[5] Protecting children from harms online - Annexes 10-15 (ofcom.org.uk), page 6
[6] Principle (c): Data minimisation | ICO
[7] Principle (a): Lawfulness, fairness and transparency | ICO

service must only process personal data in ways people would reasonably expect and which do not have an unjustified adverse impact on them. In order to make such an assessment, services need to consider whether such processing is necessary and proportionate.

The draft guidance notes[8] that the technical criterion of fairness is distinct from the concept of fairness in the UK GDPR. In our view the fairness criterion outlined in Annex 10 should align with the requirements of fairness under data protection law so that services are clear that the requirements across the regimes are consistent. We made a similar point in our response to the consultation on the Part 5 guidance.

Age Assurance Measures AA1-6 (Volume 5, section 15, Annex 7 section H)

The requirement for age assurance to be 'highly effective'

As volume 5 makes clear, s12(6) of the OSA requires 'highly effective' age assurance to be used to prevent children from encountering primary priority content (PPC) that is harmful to children (s12(3)(a)).

The OSA itself does not have a requirement that age assurance that is used to protect children from priority content (PC) should be 'highly effective'. However, Ofcom explains that it has exercised its judgment to go beyond the strict requirements of the legislation and recommend 'highly effective' age assurance for measures related to PC. At paragraph 15.309 of volume 5 of the consultation documents, Ofcom explains this decision by saying "based on current evidence, we do not believe that it would be feasible to specify an alternative level of effectiveness that is clearly distinguishable from highly effective age assurance and that would still achieve a sufficient level of protection for children relative to the risk of harm".

We do not challenge Ofcom's proposal that it is appropriate and proportionate to recommend the use of 'highly effective' age assurance to protect children from PC for the purposes of compliance with s12(2) and (3) of the OSA. Ofcom provides robust information about the likely risks and impacts presented by such content to justify its approach (in volume 3 of the consultation documents). That being said, it will always be important that 'highly effective' age assurance is not implemented in a disproportionately intrusive manner. Services who use 'highly effective' age assurance to comply with the online safety duties for both PPC and PC should be able to demonstrate that the approach they use complies with

[8] Annex 10, page 15, footnote 17

data protection law. We provide more information about this in our response to Annex 10 above.

Age assurance to differentiate children of different ages

Ofcom is not proposing the use of age assurance to determine the age groups of users below the age of 18. We do not question the appropriateness of focusing measures AA1-6 on differentiating between over and under 18s. The OSA requires services to prevent children of any age from encountering PPC and it would therefore not be necessary or proportionate for services to differentiate between child age groups for the purposes of complying with s12(3)(a) OSA.

In relation to PC, although the OSA envisages that measures should be tailored to age groups judged to be at risk of harm, we note Ofcom's view that there is currently limited evidence on the specific impact of harms to children in different age groups (vol 5 paragraph 15.317) and that its current focus is on establishing recommended protections for all children under 18 rather than tailoring protections for particular age groups (15.319). We also note that Ofcom may look to adjust its recommendations on PC to focus on specific age groups in the future.

Ofcom also concludes that there is currently limited independent evidence about the capability of existing age assurance methods to correctly distinguish between child users of different age groups to a 'highly effective' standard, without disproportionately affecting children's rights (15.318). This limitation is one of the reasons Ofcom provides for not tailoring protections for children in different age groups (15.319).

This assessment should not disincentivise services from using age assurance to determine a child's age for the purposes of complying with data protection law and conforming to the standards of the Children's code that provide for age-appropriate application. We appreciate that this is not Ofcom's intention and we note that the draft risk assessment guidance envisages the voluntary use of age assurance to apply minimum age requirements[9]. We do however ask that Ofcom clarifies its position more explicitly.

Specifically, it should clarify that its assessment relates solely to whether age assurance solutions satisfy the 'highly effective' criteria that it applies to the online safety regime and that it is not making a general statement

[9] Annex 6, Draft Children's Risk Assessment Guidance, paragraph 4.46: "Service providers should be mindful of underage users who may access their service despite specific age limits set out in their terms of service, unless they use a form of highly effective age assurance to enforce age limits."

that age assurance solutions are currently incapable of detecting the age or age group of a child accurately.

We agree with Ofcom that age assurance solutions are developing rapidly, and we anticipate that solutions that are capable of accurately assessing age with increasing levels of granularity will become more prevalent. However, we stress that organisations should not take Ofcom's current position to mean that it is not currently possible for them to take age assurance steps to comply with their responsibilities under data protection law.

Age assurance and proactive technology

The OSA Schedule 4(13) constraint on Ofcom's powers to recommend the use of proactive technology where content is communicated privately provides an important privacy safeguard.

We recognise that the user-to-user (U2U) code of practice does not recommend that services use proactive technology to comply with the age assurance measures (which apply to both public and private communications). However, the section of Volume 5 describing current practices in age assurance features several descriptions of apparent user profiling technology, including a machine learning model used by Google which infers whether a user is over or under 18 "based on a variety of behavioural signals" (15.35, page 42).

We are concerned that the inclusion of such examples, without contextualisation, could encourage some services to use proactive technology, such as user profiling or behaviour identification techniques, for age assurance where content is communicated privately because they think that the measure requires it. We therefore recommend that Ofcom clarifies why it has included examples of this nature and clarifies that where proactive technology forms part of a service's age assurance function, it is not making a recommendation for the use of proactive technology where content is communicated privately.

Content moderation (Volume 5 section 16, Annex 7 section B)

Content moderation systems deployed by U2U services often involve the processing of people's personal data.

In most cases, user-generated content in a service's moderation systems is likely to be personal information. This can be because:

- the information is about someone (for example, where the content contains information that is clearly about a particular user); or

- it is connected to other information, making someone identifiable (for example, the account profile of the user who uploaded it, which may include information like their name, online username and registration information).

Beyond the content itself, content moderation may also involve using personal information that is linked to the details of a user's account or profile. For example, this can include a user's age, location, previous activity on the service, or a profile of their interests and interactions.

We have published guidance for U2U services setting out our data protection expectations for content moderation. This includes guidance on how services can ensure that they protect children's information rights when carrying out content moderation. In particular, the guidance highlights that services carrying out content moderation that involves children's personal data must:

- Conduct a data protection impact assessment (DPIA).
- Take extra care to protect children's interests if they are relying on the lawful basis of legitimate interests.
- Provide information to users in a way that is accessible and easy for children to understand.

We are committed to working with Ofcom to ensure that the online safety and data protection regimes are aligned and that organisations understand how data protection and online safety requirements interact in relation to content moderation.

Content moderation and proactive technology

As noted in relation to the age assurance measures, OSA Schedule 4(13) prevents Ofcom from recommending the use of proactive technology (including content identification technology) to analyse user-generated content communicated privately, or metadata relating to user-generated content communicated privately, in a code of practice. This is an important safeguard for user privacy.

We recognise that Ofcom has not included specific recommendations that services use content identification technology[10], or any other type of proactive technology, to comply with the content moderation measure in the U2U code. However, as noted on page 103 of volume 5, large services with a substantial amount of content may rely on automated content moderation tools to ensure that moderation of content harmful to children is scalable and efficient. Services may therefore voluntarily choose to use

[10] OSA s231(2): '"Content identification technology" means technology, such as algorithms, keyword matching, image matching or image classification, which analyses content to assess whether it is content of a particular kind (for example, illegal content).'

content identification technology as part of the content moderation process that they put in place to comply with measure CM1.

Measure CM1 applies to both content that is communicated publicly and privately. Where a service incorporates content identification technology into their content moderation processes, there is a risk that they may assume that measure CM1 requires them to deploy content identification technology on content that is communicated privately. In accordance with the spirit of the restraint in Schedule 4(13) we recommend that Ofcom specifically clarifies that where content identification technology forms part of a service's content moderation function, the service is not required by measure CM1 to use content identification technology in relation to private communications on the service.

We note that Ofcom is planning an additional consultation on how automated detection tools can be used to mitigate the risk of content harmful to children and illegal content and we look forward to responding in due course.

Performance targets related to speed and accuracy (CM3)

Measure CM3 requires that large or multi-risk services likely to be accessed by children should set and record performance targets for their content moderation function. In the U2U code, measure PCU B3.4 provides that, in setting its targets, the provider should balance the desirability of taking content harmful to children down swiftly against the desirability of making accurate moderation decisions. At paragraph 16.122 of volume 5, Ofcom acknowledges the risk that setting performance targets can lead to a focus on speed rather than accuracy, which could interfere with users' right to privacy. Ofcom says that it has designed the measure so that services will need to balance speed with the degree of accuracy, which it thinks will mitigate the risk of unjustifiable interference with users' rights. It does not propose to stipulate the performance targets that services should set.

We support the principle of setting and recording of performance targets. For example, accuracy targets could safeguard privacy if they make systems more accurate and hence fairer. However, the measure does not provide guidance for services about what a desirable balance between accuracy and speed would be. The accuracy principle in data protection law means services must take all reasonable steps to ensure the personal information they use and generate through their content moderation processes is not incorrect or misleading. We provide more information about content moderation and data protection accuracy in our content moderation guidance.

We therefore suggest that paragraph PCU B3.4 provides that, in setting targets, services should be mindful of and comply with the requirement in data protection law to take all reasonable steps to ensure the personal information they use and generate through their content moderation processes is accurate. This suggestion also applies to recommendation SM4 of the children's safety code of practice for search services (Annex 8, PCS B4.4).

Search moderation (Volume 5 section 17, Annex 8 section B)

We understand that the search content moderation measure recommended by Ofcom does not require services to process personal data relating to users in order to identify search content that is harmful to children. However, as Ofcom acknowledges in its privacy rights assessment[11], the measure may be implemented in such a way that personal data would need to be processed in order to facilitate the measure (for example, where a service chooses not to apply the measure to verified adult users). We welcome that Ofcom has referred to the need for services implementing this measure to comply with data protection law.

User reporting and complaints (Volume 5 section 18, Annex 7 section C)

Appropriate action in response to age assurance complaints (UR4c)

Measure UR4c(i) includes a requirement that services likely to be accessed by children take appropriate action in response to complaints about incorrect assessment of a UK user's age where measures AA3-6 apply. Services are required to reverse any restrictions to user access to content that is applied as the result of incorrect age assurance. They are also required to monitor trends in complaints about incorrect assessments of age and use this information to help ensure that the age assurance method fulfils the criteria for 'highly effective' age assurance.

However, measure UR4c(i) does not apply to services which apply the user access measures at AA1-2. In other words, there is no recommended measure applying to AA1 and AA2 that requires services to put in place a complaints mechanism to enable adult users to make complaints about incorrect assessment of age. Nor is there a requirement on services to take appropriate action in response to such complaints or to monitor age assurance complaints trends.

In its privacy rights assessment for measure AA1[12], Ofcom points to the ICO's guidance in the Opinion that "services must provide tools so that

[11] Volume 5, paragraph 17.99
[12] Volume 5, paragraph 15.79

people can challenge inaccurate age assurance decisions" and suggests that this is a way that services can mitigate the negative impact arising from incorrect assessments of age under AA1 and by implication AA2. The reference to the Opinion is correct. The requirement is based on the data protection fairness principle and the right to rectification which provides that data subjects have the right to obtain the rectification of inaccurate personal data[13]. We consider however that simply signposting to data protection law within the rights assessment could easily be overlooked by services and users.

We recognise that data protection law does have the requirement for services to put in place a mechanism to challenge inaccurate age assurance decisions. However, we think that Ofcom is in a better position to set out what an effective redress mechanism for these specific measures would be. We recommend that Ofcom amends its code of practice so that services which apply user access measures AA1-2 are also required to implement measure UR4c(i). This would align with data protection law whilst also providing a redress mechanism that is bespoke to the age assurance measures recommended by Ofcom.

Terms of service enforcing minimum age restrictions (Annex 7, measures PCU D1.2(d) and PCU D1.3)

The above code measures essentially transpose the duty in s12(11) of the OSA that provides that if a service provider chooses to take or use a measure designed to prevent access to the whole or part of the service by children under a certain age, the service provider must include provisions in the terms of service specifying details about the operation of the measure and must apply those provisions consistently.

In our view the language of the OSA and of the corresponding code measures is ambiguous in that it is not clear what the requirement that services must "apply the provision consistently" means services should do in practice. We would welcome more clarity about this.

We note that these draft measures do not incorporate safeguards for privacy. S49(2)(b) OSA makes clear that the "safe harbour" for compliance with the s22 OSA duty to have particular regard to the importance of protecting users from a breach of privacy law is only relevant where a measure contains privacy safeguards. On our reading, the safe harbour would not therefore be available to a service that applies measures PCU D1.2(d) and PCU D1.3. This means that services will need to ensure that they take specific steps to comply with their s22 OSA duty. We recommend that Ofcom considers this point and makes this clear to services.

[13] UK GDPR Article 16

User support measures (Volume 5 section 21, Annex 7 section E)

User support measure 5 (US5): Signposting child users to support

Ofcom makes a number of recommendations that focus on making supportive information available to children in relation to suicide content, self-harm content, eating disorder content and bullying content and helping them to understand what action they can take if something goes wrong. The measures apply at three intervention points (when children report content, when children post or repost content and when they search for user-generated content on U2U services). Volume 5 sets out evidence to suggest that signposting is effective for these specific categories of content and at the specified intervention points. We also note that intervention points 2 and 3 only apply where a service already has measures that enable them to identify relevant content. Services are not therefore incentivised to carry out additional monitoring of content or searches to implement these measures.

In principle we support the inclusion of signposting measures in the codes of practice, and we do not question the proportionality of the scope of the measures. The objective of the measures aligns with standard 13 of the Children's code which suggests that services may wish to consider using nudge techniques in ways that support children's health and wellbeing. The Children's code also makes clear that if services use personal data to support signposting features, they need to make sure their processing is compliant (including providing clear privacy information) but that, provided that other data protection requirements are met, the related processing is likely to meet the data protection fairness requirement.

We are pleased that Ofcom's approach is consistent with the ICO's Children's code and that it has directed services to the need to comply with data protection requirements. We suggest that services should also be reminded that they may be processing special category data[14] in connection with these measures, especially in relation to information about a person's general or mental health, and services should consult ICO resources about how to do this in compliance with data protection law.

Search features, functionalities and user support (Volume 5 section 22, Annex 8 section E)

Search support measure 2 (SD2): Provision of crisis prevention information

This measure requires large general search services to provide crisis prevention information in response to search requests regarding suicide,

[14] Special category data | ICO

self-harm and eating disorders. Depending on how services implement these warnings, this could result in services processing personal data to deliver warnings to individual identifiable users, and as a result processing of user personal data could occur when search terms are analysed. Analysing searches to provide crisis prevention information may also require services to process special category data relating to the health of users.

A similar measure around the provision of crisis prevention information in response to search requests regarding suicide was proposed in Ofcom's illegal harms search code of practice. In our consultation response[15], we advised that the privacy assessment did not fully set out the impact on privacy depending on how services implemented the measure, and that the importance of data protection compliance was not made clear to services. For the protection of children code recommendation, Ofcom's privacy assessment acknowledges that some services may implement this measure in a way that involves the processing of users' personal data. It also highlights the need for services to comply with data protection law where this is the case, stating that this will be key to ensuring that any interference with users' rights to privacy is proportionate and no more than necessary for services to fulfil their children's safety duties under the OSA.

We are pleased that Ofcom has put in place the changes we recommended. We suggest that services should also be reminded that they may be processing special category data[16] in connection with these measures, especially in relation to information about a person's general or mental health, and services should consult ICO resources about how to do this in compliance with data protection law.

User control measures (Volume 5 section 21, Annex 7 section G)

Measure US1: Provide children with an option to accept or decline an invite to a group chat

The measure is designed to prevent children being added to group chats by others when they do not want to be. This is an outcome that the ICO supports. Standard 7 of the Children's code[17] requires settings to be "high privacy" by default (unless the service can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child). Privacy settings are a practical way for services to offer children a choice over how their personal data is used and protected.

[15] ICO response to Ofcom OSA illegal harms consultation, page 21.
[16] Special category data | ICO
[17] 7. Default settings | ICO

We do, however, note that the measure carries a potential risk that the fact that a user is a child will be revealed to other users in the chat. This is because the measure requires services to take specific actions when a child user is added to a group chat that they are not required to take for adult users. We welcome that Ofcom has recognised this risk in its privacy rights assessment, and that it has advised services to take steps to mitigate the potential concern, as well as highlighting the need for services to comply with data protection law. Services should conduct a data protection impact assessment to ensure that risks arising from the processing are identified and mitigated, and follow a data protection by design and default approach to the design and implementation of the measure. We are happy to work with Ofcom to consider practical and privacy-friendly solutions.

Recommender systems (Volume 5 section 20, Annex 7 section F)

The use of children's personal data in recommender systems is an area of focus for the ICO's current Children's code strategy[18]. As both the ICO and Ofcom have a regulatory interest in this area, our ongoing collaboration will continue to be important in ensuring that children are protected from the content and data protection harms that can arise from recommender systems.

Relevant available information

Ofcom's proposed recommender system measures specify that services should identify and use relevant available information to identify content likely to be PPC or PC. Where relevant available information is personal data, services will need to ensure that they comply with data protection law, as Ofcom has recognised.

Compliance with the data minimisation principle[19] will be important for ensuring that any processing of personal data is compliant with data protection law [20]. For example, user reports about content are likely to contain personal data, but it is unlikely that the full content and context of the user report will always be required to identify PPC or PC within a recommender system. Services should therefore look to remove personal data from the relevant available information used to facilitate this measure as much as possible. Where it is necessary to process some personal data, services should aim to anonymise, pseudonymise or minimise the quantity of personal data processed in the performance of this measure. Services will also find it useful to consult the ICO's guidance

[18] Protecting children's privacy online: Our Children's code strategy | ICO
[19] Principle (c): Data minimisation | ICO
[20] How do we ensure data minimisation in our content moderation? | ICO

on content moderation for information about our expectations for services that process personal data to identify violative content.

We respond below to the draft guidance on content harmful to children and our observations about the consideration of contextual factors in relation to that assessment apply equally to the recommender systems measures.

Rights assessment for code of practice for U2U services - Privacy (Volume 5)

In places the privacy rights assessments for measures AA1-6[21], CM1[22], UR1[23] and RS1[24] of the code of practice for U2U services appear to conflate legitimate expectation of privacy considerations with data protection rights. For example, they suggest that the degree of interference on data protection rights will depend on whether the content affected by a measure is public or private. This is not accurate under data protection law and is primarily a matter concerning reasonable expectations of privacy. It is also not always clear what Ofcom considers to be the specific data protection impact. One option would be for the impact assessments to differentiate the privacy analysis from the analysis of data protection impacts, for example by including "data protection impact" as a separate sub-heading. However, we agree with the overall conclusion that compliance with data protection law contributes to ensuring that the recommended measures are proportionate.

Section 2: Children's Risk Assessment Guidance volume 4 and Annex 6

[21] Measure AA1: Use HEAA to prevent children accessing services whose principal purpose is the hosting or dissemination of PPC, Volume 5 paragraph 15.73
Measure AA2: Use HEAA to prevent children accessing services whose principal purpose is the hosting or dissemination of PC if the service is also high or medium risk for PC, Volume 5 paragraph 15.100
Measure AA3: Use HEAA to prevent children's access to PPC on services that do not prohibit PPC, Volume 5 paragraph 15.157
Measure AA4: Use HEAA to protect children from PC on services that do not prohibit PC, Volume 5 paragraph 15.195
Measure AA5: Use HEAA to apply relevant recommender system measures to protect children from PPC, Volume 5 paragraph 15.238
Measure AA6: Use HEAA to apply relevant recommender system measures to protect children from PC, Volume 5 paragraph 15.264
[22] Measure CM1: Content moderation systems and processes designed to swiftly action content harmful to children, Volume 5 paragraph 16.57
[23] Measure UR1: Have complaints processes which enable people to make relevant complaints for services likely to be accessed by children, Volume 5 paragraph 18.41
[24] Measure RS1: Recommender systems to filter out content likely to be PPC from recommender feeds of children, Volume 5 paragraph 20.67

Core and enhanced inputs (volume 4, Table 4.1)

As part of step 2 of the risk assessment process, services are required to use core and, where appropriate, enhanced inputs to assess the risks of harm. The core and enhanced inputs are likely to involve processing of personal data. For example, this could include data from user complaints and reports, and relevant user data including age. We are pleased that Ofcom makes clear that any use of users' personal data will require services to comply with their obligations under UK data protection law (for example in Table 12.3 of Volume 4).

A key data protection consideration when processing personal data for risk assessment is the data minimisation principle.[25] This requires the personal data that services process to be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. This means that services should identify the minimum amount of personal data they need to fulfil their purpose. Where possible, services should ensure that personal data is anonymised, or pseudonymised to reduce the potential for it being linked to a particular person. This is referenced on page 82 of Volume 4. We would recommend that it is also included in the guidance itself (Annex 6).

Particular care is required when services process children's personal data to carry out children's risk assessments and there are also additional requirements for special category data.

Section 3: other guidance

Guidance on content harmful to children (volume 3)

Contextual factors

When determining whether content falls within the definition of PPC or PC, Ofcom recommends that services consider contextual factors related to the nature of the content or how it is presented. Ofcom explains, at paragraph 8.1.22, that this could include information reasonably available to the service provider, such as information about the user who shared the content in question or how it has been shared. This information may be personal data. Where services believe that processing personal data is necessary to identify whether content on their service is PPC or PC, they must ensure that they comply with duties under UK GDPR, UK data protection law and conform to the Children's code where it applies.

In circumstances where services deem the processing of personal data as necessary to identify whether content is PPC or PC, it is particularly

[25] Principle (c): Data minimisation | ICO

important to comply with the data minimisation principle. To demonstrate compliance, services should only collect personal data that they actually need, periodically review stored data and delete any unnecessary information. As highlighted in our response to Ofcom's recommendations on recommender systems (see above), services using relevant available information to inform whether content is PPC or PC should aim to anonymise, pseudonymise or minimise the quantity of personal data processed.

The rights assessment at paragraph 8.50 does not address impacts on rights to privacy or data protection because it notes that the guidance is not recommending that services process or retain any particular kinds of personal data. We suggest that this is reconsidered in the light of our above observations. The impact on data protection rights that may arise from consideration of contextual factors should be taken into account.

Draft children's access assessments guidance (Annex 5)

Under the online safety regime, the children's access assessment is a process for establishing whether a service is likely to be accessed by children under Chapter 4 of the OSA. We are pleased that the guidance makes it clear that the online safety requirement for services to carry out an assessment is separate to the assessment that services should carry out to decide whether they are in scope of the Children's code[26]. We agree with Ofcom that services may be able to use evidence provided for one assessment to help support the other.

ICO data protection guidance sets out a non-exhaustive list of factors that could help information society services to decide whether their services are likely to be accessed by children for the purposes of the Children's code. The factors are broadly the same as those outlined by Ofcom which should help services to be efficient when completing the assessments across both of our regimes.

[26] 'Likely to be accessed' by children – FAQs, list of factors and case studies. | ICO