The Information Commissioner's response to Ofcom's Consultation on Technology Notices to deal with terrorism and CSEA content, and Draft Guidance on the exercise of Ofcom's functions under Chapter 5 of Part 7 of the Online Safety Act 2023

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), the Freedom of Information Act 2000 (FOIA), the Network and Information Systems Regulations 2018 (NIS), 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.

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 recognise the serious concerns surrounding child sexual exploitation and abuse (CSEA) and terrorism related content on online services, and the need for services to implement proportionate measures to deal with it. Ofcom's Technology Notice powers will play a crucial role in tackling these harms by requiring online services to identify and/or prevent access to such content.

We anticipate that the technologies that will fall in scope of these powers will involve processing of personal information, and we expect the technologies to be designed and deployed in full compliance with data protection law. We expect organisations to take into consideration data protection by design and default by putting in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights.[1] In some cases, these technologies may also involve storing information, or accessing information stored, on a user's device. Where technologies in scope of these powers involve the use of storage and access technologies, services must comply with the requirements of PECR.

We welcome the opportunity to respond to this consultation. Our response sets out some general observations and some more specific comments about the proposals for audit-based assessment and the draft guidance on the exercise of Ofcom's functions (consultation questions 1 and 5).

General comments

We consider the Online Safety Act's (the 'Act') requirement for technology to be accredited as meeting minimum standards of accuracy to be a crucial safeguard for privacy. Ofcom's powers to issue a Technology Notice under section 121 of the Act are significant and could impact on users' rights, including the right to privacy and the rights protected under data protection

[1] Data protection by design and default | ICO

law. Data protection law ensures that personal information is handled in ways that respect individuals' rights and freedoms. Among other requirements personal data must be processed in ways that individuals would reasonably expect and not in ways that could cause unjustified harm. This is the data protection fairness principle[2]. The data protection accuracy principle requires that personal data must be accurate, up-to-date, and rectified if necessary. Personal data should not be misleading or incorrect because inaccurate data can lead to unfair consequences for individuals[3].

The ICO enforces the law in relation to data protection. While we are not suggesting that Ofcom should accredit technologies against data protection principles specifically, there is a link between the minimum accuracy standard stipulated in the Act and data protection compliance. A robust minimum standard of accuracy should support compliance with the data protection fairness and accuracy principles and mitigate adverse impacts on individuals. An example of an adverse impact that the minimum accuracy standard should safeguard against is the risk that an individual is incorrectly associated with terrorist or CSAM content because of a false positive result produced by an accredited technology. On the other hand, a less robust minimum accuracy standard may impede data protection compliance and cause unjustified harm to individuals.

In the light of the synergy between the minimum standard of accuracy and data protection law, our starting point is that the accuracy standard should be robust, the assessment process should include independent evaluation of the evidence that an applicant provides and a decision to accredit a technology should be supported by a convincing evidence base. We would have concerns if the approach to the initial accreditation were informed by the view that the standard is only intended to be a starting point, with further consideration of the accuracy of a technology being left to the time of issue of a Technology Notice. We think it is important to maintain the robustness of the standard in its own right because, once a technology becomes accredited, it is our understanding that a Technology Notice can be

[2] ICO Guidance on Data Protection Principles (Fairness)
[3] ICO Guidance to Data Protection Principles (Accuracy)

issued without any mandatory requirement for its accuracy to be further assessed.

We note that Ofcom plans to undertake further work to determine how the accreditation scheme will work, which may include commissioning further external research. We hope that our response will assist this work.

Overall points

Stress testing

We note that there is no indication from the consultation documents that stress testing of the proposed models has been conducted at the current time. Stress testing would show how robust and effective the proposed models are in practice and might reveal sensitivities to technical and operational issues that affect the performance of the models and the assessment outcomes. As outlined above, an accuracy standard that is supported by a robust accreditation process is more likely to be compatible with data protection law.

We therefore suggest that Ofcom considers conducting stress tests as it refines its accreditation models. This will help to reveal potential unintended consequences. For example, testing may show whether a technology could be accredited despite weak overall performance or fail accreditation despite being fit for purpose overall. Stress testing of the proposed thresholds for Independent Performance Testing could reveal adverse outcomes such as the risk of accrediting a technology based on its ranking when it does not perform to an objectively high standard or creating a situation where well designed and well performing technologies may not make the ranking threshold.

In this response we have sought to provide helpful suggestions based on available information. However, we are not able to give a definitive assessment of the potential data protection concerns arising from the consultation proposals in the absence of evidence about the impact of technical and operational sensitivities on the proposed models. Our comments below are therefore made subject to that caveat.

Independent evaluation

We agree with Ofcom that independent evaluation is a necessary component of the accreditation process and that self-certification will not provide a robust assessment that technology has met the minimum standards of accuracy. The consultation documents suggest that the audit-based assessment will include an element of independent evaluation of the evidence provided by an applicant to inform the numerical scoring. Whilst we welcome this, the documents do not explain what the independent evaluation will consist of nor how the evaluation will feed into the numerical scores that are awarded. It is important that there is a meaningful independent assessment of the evidence provided and we would welcome more detail as Ofcom's thinking develops. If independent evaluation were thoroughly embedded into the audit-based assessment, it could make an additional independent performance testing stage unnecessary, but we are unable to provide a definitive view about this without more information.

If implemented effectively, independent evaluation would avoid a technology being accredited solely on paper without meaningful interrogation. Otherwise, there is a risk that technologies with well-documented but suboptimal performance appear more effective and therefore be rated more favourably than is justified by their real-world performance. Accreditation of suboptimal technologies risks causing adverse impacts on individuals when the technologies are deployed and creates the potential for non-alignment with data protection law when the technology is deployed.

We would also suggest that independent evaluation would enable a qualitative assessment of the evidence which could helpfully supplement the numerical scoring. Whilst we recognise that scoring offers a structured approach and can be a useful tool for ranking the effectiveness of technologies or evaluating specific metrics, a purely numerical system may not fully capture the complexities of each technology, particularly in relation to its real-world application and potential limitations. Issues such as inaccurate reporting, unfair outcomes, or unintended biases may require deeper analysis beyond a numerical scoring framework. The scoring system also risks being inflexible if it does not adequately account for the nuanced

trade-offs between different evaluation criteria. Too much rigidity could allow some technologies to achieve a pass score despite significant weaknesses.

We therefore look forward to engaging further with Ofcom about the form of independent evaluation that is envisaged.

Policy proposals for minimum standards of accuracy for accredited technologies

Question 1: Do you have any views on our audit-based assessment, including our proposed principles, objectives, and the scoring system?

Audit-based assessment (paragraphs 4.13 - 4.19)

Proposed scoring principles

We broadly agree with the proposed principles (technical performance, fairness, robustness, and maintainability) and recognise the importance of these principles in ensuring accuracy of CSEA and terrorism detection technologies. Demonstration of the audit principles may also support compliance with the data protection accuracy and fairness principles.

Measuring statistical accuracy

We note that it is Ofcom's provisional view that the minimum standards of accuracy should consider technical accuracy in its 'widest sense', using a range of metrics which give complementary insights into the technology's performance. We agree with the conclusion that accuracy could encompass a variety of performance metrics for the purposes of minimum standards of accuracy.

In principle, Ofcom's approach aligns with the ICO's guidance on AI and data protection[4] which makes the following comments in relation to statistical accuracy and how that relates to data protection accuracy and fairness. In that guidance we note that "overall statistical accuracy is not a particularly useful measure and usually needs to be broken down into different measures". We make the point that it is important to identify, measure and

[4] ICO's Guidance on AI and Data Protection: What do we need to know about accuracy and statistical accuracy?

prioritise the right metrics based on the specific application of the technology.

The ICO guidance also acknowledges that there are trade-offs between precision and recall. It recognises that false positives and false negatives can have significantly different consequences for individuals, which, in turn, can impact the fairness of personal information processing under data protection law. The guidance says that services should prioritise avoiding specific types of errors based on the severity and nature of the associated risks.

In relation to technologies that will be in scope of Ofcom's Technology Notices powers, the consequences of false positives are likely to be significant. As noted in Ofcom's draft guidance on the exercise of its functions, false positives could lead to users wrongly having their content removed, their accounts banned or suspended, or being reported to the National Crime Agency or other organisations. Such outcomes could have a substantial impact on individuals' rights to privacy and freedom of expression including potential data protection harms. The accuracy principle requires that services take all reasonable steps to ensure that the personal data they process is not incorrect or misleading as to any matter of fact. Where decisions could have significant adverse impacts on individuals, services must be able to demonstrate that they have put sufficient effort into ensuring accuracy.

Whilst we acknowledge that the weighting attached to the false positives may vary depending on the severity and nature of the associated risks and whether the risks can be mitigated on deployment, we would expect the false positive rate to be a mandatory performance metric at all stages of the accreditation process (including the audit assessment process) to ensure that it is considered.

Without mandatory evaluation of false positives, there is a risk that technologies could be accredited despite generating a high number of incorrect classifications, which could lead to unjustified adverse effects on individuals. We therefore recommend that Ofcom clarifies how false positives will be integrated into the audit assessment process. Having mandatory data about false positives will also enable Ofcom to identify when mitigation

measures – such as requiring human review – will be necessary to address what would otherwise be an unacceptably high false positive rate.

Development in a secure environment (4.30)

We welcome Ofcom's inclusion of an accreditation objective that requires technology to be developed in a secure environment with sufficient cybersecurity, privacy and data protection measures in place. The objective refers to documentation showing how secure design principles have been followed. Relevant documentation could also include appropriate evidence of how data protection by design has been complied with under Article 25 of the UK GDPR. We suggest that we engage further with Ofcom this point to ensure that the documentation fully aligns with the assessment objective.

We are also pleased to note that the Impact Assessment in Annex 7 of the consultation documents states that Ofcom would reserve the right to consider a technology where it is found by the court or a competent authority such as the ICO to have been developed in breach of UK data protection requirements. This is restated in footnote 62 of the consultation document. We suggest that it should be set out more prominently in the final version of the accreditation documents to avoid it being overlooked.

Lack of clarity about the Audit Assessment scoring criteria

In relation to the scoring criteria, it is currently unclear what will constitute "robust and comprehensive evidence" and "limited evidence" in practice, which would leave the consistency and transparency requirements in the scoring system open to interpretation. Without clear definitions and standardised criteria, there is a risk that scoring could be applied inconsistently, leading to uncertainty about how technologies are evaluated. The consultation documents explain that Ofcom will provide a list of the audit assessment questions in due course in part to ensure a consistent approach to scoring. As part of this, we suggest that Ofcom considers developing guidelines on what would qualify as robust or limited evidence to support consistency.

Question 5: Do you have any comments on our draft Technology Notice Guidance?

We have the following observations on the draft Technology Notice Guidance.

Data protection compliance and Technology Notices

As noted above, we expect that the technologies that are in scope of a Technology Notice will involve the processing of personal information. Such processing must fully comply with data protection law. We suggest that the guidance explicitly informs companies of this requirement to make it clear that companies cannot avoid their data protection obligations merely because the personal information processing is required to comply with a Technology Notice.

Before issuing a Technology Notice, Ofcom is required to evaluate the level of risk of the use of the technology resulting in a breach of privacy and data protection law. This is one of the Specified Matters that Ofcom must consider when deciding whether it is necessary and proportionate to issue a Technology Notice. The draft guidance does not specify how Ofcom will take the level of risk or the likelihood of a data protection breach into account when deciding what is necessary and proportionate. Ofcom should make clear when it expects to consult the ICO prior to issuing a Warning or a Technology Notice to mitigate the risk of a breach of data protection law. It is important that a Technology Notice is not incompatible with data protection compliance. The ICO stands ready to provide its expertise as part of the joint commitment with Ofcom to maximise coherence and promote compliance across both of our regimes.

Section 125(5) of the Act

Section 125(5) of the Act states that a notice given to a provider of a regulated service, requiring the use of accredited technology, is to be taken to require the provider to make such changes to the design or operation of the service as are necessary for the technology to be used effectively[5]. The Explanatory Note to the Act clarifies this provision by explaining that the company must make "proportionate" alterations to the regulated service to ensure that the specified technology is effective when implemented.

[5] Section 125(5) of the Act and paragraph 598 of the OSA Explanatory notes

The draft guidance states that Ofcom will set out any proportionate changes to the service's infrastructure that may be needed to effectively implement the technology or (where a service provider is already using accredited technology) to do so more effectively.

The guidance also states that when issuing a Notice requiring the use of accredited technology, Ofcom would not be restricted from considering a solution technically feasible simply because proportionate changes would be required to the design or operation of the service.

We note that the draft guidance does not indicate what kinds of changes Ofcom would consider to be proportionate for the purposes of s125(5) or where it would set the threshold for changes that may be disproportionate. Nor does the guidance clarify how Ofcom interprets the meaning of a service's "infrastructure" for the purposes of a Warning Notice. In the interest of providing certainty, we suggest that Ofcom clarify its approach to these matters. We would be particularly keen for the Guidance to confirm that requiring a company to undermine or reduce technical or organisational measures that are necessary to comply with data protection law would not be a proportionate change.

Section A3: A Technology Notice must be necessary and proportionate

The matters we must consider when deciding if a Technology Notice is necessary and proportionate

We welcome Ofcom's high-level observations on its approach to Specified Matters (paragraph A3.7 of the draft guidance). With regard to A3.7(c) we are pleased that Ofcom expects to have regard to evidence regarding the false positive rate of the technology under consideration. As we note above, false positives could lead to significant adverse data protection impacts on users.

The draft guidance also indicates that Ofcom will consider any potential safeguards to mitigate the risks [arising from false positives] such as layering of measures. We are pleased to see that Ofcom is considering these safeguards as part of its decision to issue a Technology Notice. But, as noted in our comments on Ofcom's accreditation proposals, we are not confident that deferring such consideration of false positive rates to the issuing of a

notice is sufficient to ensure that robust standards of accuracy are upheld. We have already given our view that false positive rates should also form part of the metrics that are available at the stage of accrediting a technology as well as informing whether it is necessary and proportionate to give a Technology Notice in a particular case.

At paragraph 3.7(f) Ofcom notes that, in the case of a Technology Notice to develop or source technology, it typically expects to consider the Specified Matters based on the information available at the time it issues a notice for a service to develop or source technology. We welcome Ofcom's approach. But on our reading of the Guidance, there is no guarantee that Ofcom will reconsider the Specified Matters against the technology that has been sourced or developed. Given the potential risks to users' data protection rights, we feel it would be appropriate for Ofcom to carry out an updated assessment at the point of requiring deployment.

Compatibility testing

We welcome Ofcom's proposal to consider whether independent compatibility testing is appropriate to inform its decision making.

We suggest that rather than compatibility testing being something that Ofcom will consider on a case-by-case basis there should be a presumption that it will be carried out *unless there* is independent and robust evidence already available to Ofcom about the performance of the technology for the specific use case. Compatibility testing could surface issues of potential breaches of data protection law which could be mitigated in the Warning or Technology Notice. Such an approach would allow the real-world application of the technology and its potential limitations and risks to be considered before a final decision about its deployment is taken.

We also welcome that the draft guidance highlights the extent to which use of the technology would result in solely automated decision making as one of the factors that will be relevant when deciding whether compatibility testing is appropriate. Where solely automated decision-making is used, inaccurate decisions could have significant effects on individuals and compatibility testing offers a valuable safeguard against this occurrence.

Concluding remarks

There are numerous touchpoints between Ofcom’s Technology Notice powers and data protection, and we look forward to continuing to work closely with Ofcom to achieve alignment between our regimes. It's important that Technology Notices are not incompatible with data protection law.