SHOOSMITHS

6th Floor
2 Colmore Square
38 Colmore Circus Queensway
Birmingham
B4 6SH
DX 701863 Birmingham 6

T 03700 864000
F 03700 864001

alice.wallbank@shoosmiths.co.uk
T +44 (0) 7514 731 187

The Information Commissioner
Information Commissioner's Office

anonymisation@ico.org.uk

Date 13 September 2022

Delivered: By E-mail

Dear Sir

CALL FOR VIEWS: ANONYMISATION, PSEUDONYMISATION AND PRIVACY ENHANCING TECHNOLOGIES GUIDANCE

I am writing on behalf of our Privacy and Data team in response to your call for views in respect of the consultation on Chapters 1 to 4 of the Anonymisation, pseudonymisation and privacy enhancing technologies guidance ("Draft Guidance").

(For ease, I have noted typographical or stylistic comments in *italics* to separate them from substantive commentary.)

Chapter 1 (Introduction to anonymisation)

Page 13, para 4: "In general it is likely that applying anonymisation techniques to the personal data you hold will be fair and lawful". In our experience, establishing a lawful basis and dealing lawfully with personal data during the process of collection and anonymisation is one of the most challenging aspects of legal compliance. Further commentary on this aspect of processing would be extremely useful to practitioners.

Page 16, boxed example, final para: "Both parties need to carefully assess the status of the data in the hands of the second organisation (ie whether from their perspective they could regard it as anonymous information)." The reference to a "second organisation" might more helpfully be expressed as a "third party organisation" to maintain consistency with the earlier reference.

Page 18, final para: "**individual rights** – employing pseudonymisation techniques may reduce the amount of data you have to consider when responding to requests from individuals. For example, if your purposes for processing do not or no longer require identification of individuals, you are not required to process additional information in order to do so (or to comply with other requirements of data protection law). So, where you can demonstrate you are not in a position to identify individuals, the rights of access, rectification, erasure and data portability do not apply. However, you need to be able to respond to these requests if individuals provide you with additional information that enables

their identification." This paragraph contains potentially valuable guidance but as expressed is somewhat difficult to follow. Clarification would be welcome.

Chapter 2 (How do we ensure anonymisation is effective)

Pages 4 to 7 passim: This passage will be key to helping users understand how the concept of individuation relates to the application of data privacy law. One question which has proved difficult to navigate is the extent to which any data which includes identifiers, but only ones which are practically impossible to link to a known individual, constitutes anonymous data. This may be particularly relevant to technologies which can assign a unique identifier to individuals for the purposes of processing where the identifier can never be linked back to a known individual. The Draft Guidance is not quite consistent on this point. For example, "At the same time, the existence of identifiers does not always mean that individuals are identified or identifiable (para 8) and "whether any potential identifier actually means an individual is identifiable depends on the context" (para 3) would both suggest that the presence of identifiers does **not** in itself predicate personal data. However, "Essentially, if you can distinguish an individual from other individuals, then they are identified or identifiable" (para 2), and "In most cases, a unique identifier will mean you can distinguish someone from someone else. For example, an NHS number is different for every individual and therefore will allow them to be singled out from other individuals in the dataset" (page 5 para 3), and "even if you do not intend to take action about an individual, the fact that they can be singled out may allow you to do so" (page 6 para 4) all tend to advance the contrary view. Further clarification or guidance on this issue would be welcome, even if such guidance only extends to a clear exposition of the problem and acknowledgement of the difficulties in expressing a settled position.

Page 4, para 5: "However, as detailed above, the definition also specifies other factors [such] that can mean an individual is identifiable[.]." Suggested typos are noted in square brackets.

Page 6, para 9: "In turn, this means the information in question **is** personal data that has undergone pseudonymisation, rather than anonymous information" (my bold). This proposition might be more accurately expressed by replacing the word "is" (indicated in bold) with the words "may be".

Page 7, para 3:" Whether an inference is personal data depends on whether it relates to an identified or identifiable individual." I would suggest that the intended meaning of this may in fact be "Whether an inference **results in data being treated as** personal data […]".

Page 10, para 2: "This means the status of information – as personal data or anonymous – can change over time." Here and elsewhere the Draft Guidance advances the proposition that data which it was perfectly acceptable to treat as anonymous at the time, may, due to technological advance or otherwise, become personal data. This change in status is likely to have significant practical repercussions for users. It would be useful to have additional guidance on this point, for example, whether users are likely to be given the benefit of an amnesty period or reduced compliance obligations in relation to data of uncertain or newly-changed status.

Page 14, para 5: "However, you need to: document and justify your decision; and keep this under review (eg as technologies change over time)." Guidance on the expected format of such documentation would be helpful.

Page 17, first bullet point: "nefarious". This may not be a well-understood term; suggest using "criminal purposes".

Page 20, para 6: “However, the mere possibility of making an educated guess about whether an individual is identifiable does not necessarily present a data protection risk. Even where a guess based on anonymous information is correct, this does not mean that a disclosure of personal data has happened.” This paragraph does not seem entirely consistent with other passages, given that information which carries a risk of being subject to an “educated guess” would seem to carry a high identifiability risk. Clarification or re-weighting of this would be welcome.

Page 27, diagram: There seems to be a degree of circularity about this diagram as currently conceived. For example, the box labelled “Undertake your identifiability risk assessments and anonymisation processes” would seem more logically to come **before** the box marked “is personal data involved”. Again, it is not clear whether data which is judged inherently anonymous (and therefore does not need to be anonymised) should nevertheless pass through an identifiability risk assessment.

The Identifiability Risk Assessment (passim). It would be useful to clarify the nature and role of this proposed assessment. In particular:

- References are inconsistent: it is variously referred to as an Identifiability Assessment, and Identifiability Risk Assessment.
- Is the Identifiability Assessment intended to be akin to a DPIA to be completed each time anonymisation is performed?
- Should it include features such as balancing test?
- Is the Motivated Intruder Test (page 18 et seq.) intended to form part of the Identifiability Assessment or are they two separate assessments?
- Is it the responsibility of a controller to complete the required test(s), or can it be carried out by a processor anonymising data?
- Are there additional considerations where a processor located in a third country completes the test(s)?
- A template, and further guidance on the nature and review period for the test(s) would be useful.

Chapter 3 (Pseudonymisation)

Page 2, bullet point 4: “Take care not to confuse pseudonymisation with anonymisation. Ultimately, pseudonymisation is a way of reducing risk and improving security. It is not a way of transforming personal data to the extent the law no longer applies”. The logic of the Draft Guidance means that it is difficult to establish a distinction for practical purposes between anonymisation and pseudonymisation. For example, the guidance appears to impose an ongoing duty to review anonymous data (see for example Chapter 2, page 14 para 5, and page 27) which would appear to erode the distinction.

Page 11, para 4: “However, you should remember that if you originally collected the data on the basis of consent, you usually need to get fresh consent to ensure your new processing is fair and lawful.” It would be helpful to clarify whether or not this assertion relates to “general analysis”.

Page 12, para 4: “This is particularly the case if anonymous information is less useful. However, you should carefully consider whether you can achieve these objectives using such information first.” An example to illustrate how anonymous information is less useful would be helpful to clarify this point.

Chapter 4 (Accountability and governance)

Page 6, para 9: “As long as your anonymisation is effective, subsequent use of the anonymous information is not something data protection law applies to.” This would not seem consistent with some of the guidance on ongoing review of anonymised data, for example noted above in relation to Chapter 2 pages 14, para 5, and page 27.

Page 11, first bullet point: “For example, you should […] only use anonymous information in ways individuals would reasonably expect.” Again, this is not necessarily easy to square with propositions elsewhere in the document that data protection law does not apply to anonymous data.

Page 11, para 5: “As processing anonymous information theoretically has no direct effect on any individual, it may seem unclear why individuals should know about it.” Transparency requirements in relation to the act of anonymisation is an area of extreme difficulty for users to navigate and clarity would be welcome. Given the clear statement in Chapter 1 that the act of anonymisation itself constitutes processing, further guidance on how organisations might approach the publication of a privacy notice covering the derivation and use of anonymous information would be most welcome. For example, would it be possible to clarify whether **all** the bullet points at the bottom of page 11 would apply to a general privacy notice, or only the first two?

Page 14, para 1: “If a security incident leads to re-identification of an individual from data you treated as anonymous information prior to the incident, we would not consider this as a personal data breach at the time.” Presumably this would not apply to re-identification arising from a security incident caused by the processor in question?

Page 15, final para: “This means that you should assess whether any organisation or member of the public could identify any individual from the data you are releasing.” Some refinement of this test would be useful – perhaps with a link back to other areas of the guidance where identifiability is considered in more detail.

Page 16, para 1: “The likelihood of re-identification would mean that the anonymised data would become personal data.” This final statement does not seem to flow naturally from the previous wording and some reconsideration would be helpful.

Page 16, para 4: “For example, a risk may arise if an educated guess leads to the misidentification of an individual. Available data plus individual knowledge might lead someone to believe that an innocent person was responsible for a particular crime.” It is not entirely clear, in the context of the rest of the guidance, why these examples would not relate directly to data protection law rather than another area of law.

*Page 17, para 3: “information about people who have **passed away** might not be personal data” (my bold). A more straightforward “died” might be more appropriate in the stylistic context.*

Chapter 5 (Privacy-enhancing technologies)

We hope to submit responses to the recent publication of Chapter 5 (Privacy Enhancing Technologies) when we have had the chance to consider its content. It would be useful to understand when the call for evidence in respect of this Chapter will close.

Yours faithfully

Alice Wallbank
Professional Support Lawyer
SHOOSMITHS LLP