Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

20 October 2023

CIPL Response to ICO Consultation on Draft Guidance on Biometric Data

On 18 August 2023, the UK Information Commissioner's Office (**"ICO"**) issued its draft Guidance on Biometric Data (**"Guidance"**).[1] The ICO invited the public to submit comments by 20 October 2023. The Centre for Information Policy Leadership (**"CIPL"**)[2] supports the ICO's desire to explain how data protection law applies to biometric data in biometric recognition systems, and CIPL welcomes the opportunity to submit the following comments.

Please note that CIPL is currently preparing a white paper, provisionally titled **"Enabling Beneficial and Safe Uses of Biometrics through Risk-Based Regulations,"** to be published before the end of the year. The forthcoming white paper examines various applications of biometric technologies and their associated risks and benefits, analyses the current legal landscape and trends for regulating these technologies, and urges the adoption of a risk-based approach for potential regulation and guidance. The white paper also recommends the development of a consistent and appropriate legal definition for covered biometrics. CIPL will share this document with the ICO upon its completion and public release.

1. General Comments

- **Regulations should be based on risk –** It is important to embrace a risk-based approach in biometric data laws and regulations to help assess when, where, how, and whether the use of biometric data is appropriate in a given circumstance. A risk-based approach ensures that low-risk applications can be deployed without undue restraints, that higher or high-risk applications are deployed with appropriate protections and mitigation measures, and that substantial regulatory hurdles or complete bans are reserved only for high-risk uses where effective safeguards are not available. This approach will avoid both overregulating and underregulating biometric technologies (such as facial recognition technology, which can be applied in both high- and low-risk situations).

- **Terminology & definitions –** CIPL largely commends the ICO's proposed definition of "biometric data," for it avoids common mischaracterisations of biometric data as encompassing all data about the body or as always falling within a special category of personal data. In particular, CIPL supports the ICO's effort to clarify "biometric data" for purposes of Article 4(14) of the UK General Data Protection Regulation (**"UK GDPR"**) by including a list of illustrative practical examples. That said, one aspect of the definition—viz., that covered data "allow or confirm" the unique identification of an individual—will require further clarification. The meaning and scope of "allow" is unduly broad and insufficient for organisations that must determine whether certain data is covered. As noted above, CIPL is currently working on a white paper on biometrics, which will address the issues raised by the "allow or confirm"

[1] ICO Consultation on the draft Guidance on biometric data, available here.

[2] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and over 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at https://www.informationpolicycentre.com/. Nothing in this paper should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth LLP.

standard found in the UK GDPR and the ICO Guidance. Our paper will also explore alternative definitions and provide relevant use cases and examples, which we will share with the ICO once published.

- **Accountability measures to promote responsible use of biometrics –** Any regulations concerning the use of covered biometric data must include strong accountability and data governance measures—such as transparency, purpose limitation, effective redress, and data security—that collectively mitigate the risks of using biometric data. To that end, CIPL is pleased to see that the Guidance requires a data protection impact assessment (**"DPIA"**) for any processing likely to result in a high risk to people's rights and freedoms and further provides a list of high-risk processing operations. Risk assessment and analysis of potential harms and benefits is a necessary and essential step to ensure organisational accountability and to promote privacy, security, and safety by design. Indeed, a thorough understanding of the intended uses of biometric data and the intended purposes of biometric technologies—including the uses such technologies might enable—is highly relevant and should be the foundation for any impact assessment and compliance review.

- **Privacy-enhancing technologies ("PETs") –** The ICO Guidance states that when determining whether a DPIA is required, organisations should consider whether PETs are or can be used. CIPL fully agrees that PETs can significantly advance data protection principles and help reduce privacy risks—indeed, we will be publishing a comprehensive white paper on this very topic in the coming weeks. However, CIPL recommends that the Guidance further clarify how the use of PETs may negate the need to conduct a DPIA, i.e., that the use of PETs may countervail the need for a full-blown DPIA where the employed PETs clearly reduce risk below the required risk-threshold that normally would trigger a DPIA. Such a clarification would incentivise the use of PETs by potentially eliminating an additional compliance step—i.e., a DPIA.

- **Consent and alternative bases for the processing of biometric data –** While consent is an important means for individuals to have agency over the use of their data, it may not always be the most effective way to protect individuals and mitigate the risks associated with uses of biometric data. In that regard, CIPL is pleased to see that the ICO acknowledges alternative suitable legal bases for processing biometric data (such as for the prevention and detection of unlawful acts and for research purposes) where requiring explicit consent would not be appropriate in a given circumstance. The Guidance also states that organisations must offer a suitable alternative to individuals who choose not to consent to processing special category biometric data and must ensure that individuals do not feel under pressure to consent. CIPL agrees that individuals should have access to viable alternatives, and that those who choose to opt out of the collection of biometric data should be able to do so freely and without explanation or difficulty. However, organisations should not be forced to offer substantially less secure alternatives for their products and services where an individual chooses not to provide consent. Where the use of biometrics provides the highest level of security, organisations should not be forced to provide a significantly lower level of security because of an individual's refusal to consent. CIPL recommends that, instead of requiring organisations to offer alternatives in all instances without regard to organisational security concerns, the ICO Guidance should require organisations to offer alternatives only where those alternatives do not undermine the original purpose(s) of the collection.

2. Additional Considerations

- **Regulatory sandbox –** Regulatory sandboxes assist regulators and industry alike to understand the implications of biometric data uses; they also support responsible development and deployment of biometric technologies. In that regard, CIPL commends the ICO for prioritising biometrics as a key focus area for regulatory sandboxes[3] and for holding focus group discussions with the British Youth Forum and the Citizens' Biometrics Council.[4]

- **CIPL's forthcoming white papers –** As mentioned, CIPL is currently in the process of drafting two white papers: (i) "Enabling Beneficial and Safe Uses of Biometrics through Risk-Based Regulations," and (ii) "The Emerging Landscape for the Application of PETs." We believe these white papers are highly pertinent to the ICO's ongoing consultation on its draft Guidance on Biometric Data. The forthcoming white papers will address key aspects of the consultation's subject matter and will provide valuable insights and recommendations. As part of our commitment to contributing to the regulatory process, CIPL intends to share both white papers with the ICO upon their publication.

[3] Regulatory Sandbox, "Our key areas of focus for the Regulatory Sandbox," ICO, https://ico.org.uk/for-organisations/regulatory-sandbox/our-key-areas-of-focus-for-the-regulatory-sandbox/. Also, see "ICO Seeks Sandbox Entrants for 2024", https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/10/ico-seeks-sandbox-entrants-for-2024/.

[4] ICO, Biometrics technologies, available at https://ico.org.uk/about-the-ico/research-and-reports/biometrics-technologies/; see also Events, "Biometric Technologies and data protection," ICO (1 November 2022), https://ico.org.uk/about-the-ico/media-centre/events-and-webinars/biometric-technologies-and-data-protection/.