BCLP. Client Intelligent

Insights

GETTING TO KNOW WHO: ICO DRAFT GUIDANCE ON BIOMETRIC RECOGNITION

Sep 08, 2023

On 18 August 2023, the UK's Information Commissioner's Office ("ICO") published draft guidance on biometric recognition (the "Draft Guidance") for public consultation. The Draft Guidance explains how data protection law applies when organisations use biometric recognition systems. It is also relevant for vendors of such systems and for organisations which are either controllers or processors of personal data.

The Draft Guidance focuses on biometric recognition technology, reflecting its rapid and widespread adoption for common use cases, such as building access and online identity verification.

The ICO confirms that "biometric recognition" means the use of biometric data for identification and verification. As biometric data are used for these purposes, biometric recognition systems will invariably process special category biometric data (see below for fuller explanation). This will be the case from the point that the biometric data are initially collected, and not just from the point where the data are used to identify an individual.

WHAT'S IN A NAME? PERSONAL DATA, BIOMETRIC DATA OR SPECIAL CATEGORY DATA?

When it comes to digital information relating to appearance, characteristics or behaviour, getting the terminology right can be challenging. However, this is a critical first step because only then can an organisation begin to understand its responsibilities.

- The Draft Guidance clarifies that under the UK GDPR, personal data will only be considered "biometric data" where it:

  1. relates to someone's behaviour, appearance, or observable characteristics (such as their voice pattern or fingerprints);

  2. has been extracted or further analysed using technology, and

3. *can* [is capable of] uniquely identify the individual that it relates to.

- When processing biometric data **for the purpose of uniquely identifying a living individual,** this will be considered "special category biometric data". In order to process this data, organisations must satisfy a lawful basis under both Article 6 and Article 9 of the UK GDPR.
- An example given is an online business requiring customers to prove their identity using a remote authentication process. Customers upload a scan of an official photo identity document, such as a passport, and another photo of themselves. The company then compares the two images to confirm that they are of the same person. This process involves processing **special category biometric data** in order to uniquely identify someone, i.e. matching two biometric templates generated from both photos to verify the identity of the customer.
- When processing biometric data **without** seeking to uniquely identify a living individual (even though the information is capable of being used in this way), the information is still likely to constitute "personal data" and so an Article 6 lawful basis must be satisfied.
- An example given is of a company recording calls made by its employees. The employer may be able to recognise individual staff members from the recordings but the example indicates that a digital voice recording would not be biometric data because it has not been extracted or further analysed using technology (it also follows that it would not be special category biometric data).
- The situation would be different, according to the Draft Guidance, if the company bought a voice recognition solution to transcribe audio recordings and assign them to staff members. Assuming that this involved enrolling all meeting attendees onto the system to create a biometric template of their speech patterns and comparing the recordings against these stored templates, this is biometric data. It results from specific technical processing of someone's characteristics and allows or confirms that person's unique identification. As the employer processes the biometric data for the purpose of uniquely identifying the attendees, the Draft Guidance concludes that it is also special category biometric data.

LAWFUL BASES FOR PROCESSING SPECIAL CATEGORY BIOMETRIC DATA

- The Draft Guidance confirms that in most cases, explicit consent will be the only lawful basis available for processing special category biometric data.
- As UK GDPR standard consent must be "freely given", when considering a workplace context, employers need to assess whether they can appropriately rely on employees' consent, given the inherent imbalance of power. Consent will not be freely given where employees fear adverse consequences from refusing.

- In practice, this means that organisations using biometric recognition systems must offer an alternative to their staff that is no less favourable (for instance, swipe cards for building access where individuals have chosen not to have their fingerprint or retina scanned). There may be similar challenges for organisations relying on consent from their customers or service users, particularly for public authorities.

WHAT OTHER DATA PROTECTION REQUIREMENTS APPLY?

- The ICO confirms that the use of biometric recognition systems is highly likely to trigger the requirement to complete a data protection impact assessment ("DPIA").
- Even when processing "non-special category" biometric data (i.e. without the intention of identifying an individual), organisations may still determine that their processing would pose a high risk to the rights and freedoms of individuals, given its context and purposes. In these cases, a DPIA should be completed.
- Privacy by design principles still apply. The Draft Guidance states that organisations planning to use biometric recognition technology should ask at the initial planning stage:

  1. Will our use of biometric data be a targeted and effective way to meet our needs?
  2. What alternatives to biometric data have we considered?
  3. Could any of these reasonably meet our needs in a less intrusive way?

- Organisations need to be clear about their data flows when processing biometric data, and should clearly assess their data protection "roles" (i.e. controller, processor or joint controller). Service agreements must be entered into containing all relevant terms as prescribed by the UK GDPR (in particular, Article 28).
- Appropriate security measures should be adopted to protect biometric data. The Draft Guidance confirms that organisations must encrypt any biometric data. Organisations must also conduct regular testing and reviews of their security measures to ensure these remain effective.

THE AI DIMENSION

- The ICO is clearly alive to the possibility that providers of AI solutions may wish to use customer data to train their models. Biometric recognition systems are no exception.
- Organisations are expected to establish as part of their due diligence checks whether this will occur. The Draft Guidance notes that this could lead organisations to amend their contracts (i.e. to reflect that the service provider will act as a controller when carrying out this form of processing) or even choose another provider altogether.

The consultation runs until 20 October 2023. A "second phase" (titled "biometric classification and data protection") will then follow, with a call for evidence expected in early 2024.

Please contact the authors or a member of BCLP's Data Privacy & Security team if you have any questions about your organisation's use of biometric data. You can also access our U.S. biometric regulatory developments tracker.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Geraldine Scali

London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483
