ICO PUBLISHES DRAFT GUIDANCE ON BIOMETRIC DATA

On 18 August 2023, the UK's Information Commissioner's Office (ICO) published draft guidance on biometric data and opened a public consultation seeking responses to its draft guidance[1].

The ICO's draft guidance explains how data protection law applies to biometric recognition systems and will be followed by a second phase of draft guidance in early 2024, when the ICO will call for evidence from stakeholders. The consultation on the first phase of the draft guidance will run until 20 October 2023. The draft guidance has been designed for organisations using biometric recognition systems and applies to both controllers and processors.

1 Guidance on biometric data | ICO

Key data protection concepts

Biometric data is a form of personal data under the UK General Data Protection Regulation (GDPR). The GDPR defines biometric data as *"personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic [fingerprint] data"*. Biometric data is a special kind of personal data and to be defined as such, it must meet specific requirements relating to the qualities of the data. For example, biometric data includes observable characteristics including a person's voice, their face, or fingerprints, and anything else which can uniquely identify the person to whom the data relates.

Biometric data which is used to identify an individual uniquely is included, alongside other types of sensitive personal data, as *"special category biometric data"* under Article 9 of the GDPR and is prohibited for processing unless one of a number of specific conditions for processing special category personal data applies. Other similarly sensitive data includes data which reveals an individual's racial or ethnic origin, political or religious beliefs, and health data, among others. Biometric data is only classed as *"special category biometric data"* if it is used to identify an individual uniquely, but biometric data can still be classed as special category data if it reveals sensitive personal data about an individual.

Biometric recognition

In its draft guidance, the ICO refers to "biometric recognition", a term which is not recognised by data protection law but used in industry standards to describe the use of biometric data to identify an individual uniquely. Biometric recognition can include the use of personal data, biometric data, and special category biometric data. The data may be used to identify or verify an individual or as a means of access control verification, for example using digital fingerprints to restrict access to a space to authorised people only. Biometric recognition systems may offer greater security than traditional swipe cards or PINs.

By definition, biometric recognition systems use both personal data and biometric data. The ICO has categorised the criteria defining biometric data as follows:

- The information is about an individual's physical, physiological or behavioural characteristics;
- The information results from specific technical processing;
- The information allows or confirms an individual's unique identification.

Biometric recognition systems use special category biometric data, because the purpose of a biometric recognition system is to identify uniquely an individual using biometric data.

Data protection when using biometric data

Organisations using biometric data must comply with data protection law as biometric data is a type of personal data, and organisations must be able to demonstrate how they comply. Any systems used must be designed with the protection of personal data carefully considered, including whether processors will provide sufficient guarantee of the measures used for data protection. Organisations should carry out a Data Protection Impact Assessment (DPIA) before using biometric data. When assessing the use of biometric data and its compliance with data protection law, organisations should consider whether:

- the use of biometric data would be a targeted and effective way of meeting relevant needs;
- alternatives to the biometric data could be considered;
- any of these could meet the relevant needs in a less intrusive way.

For any processing which is "likely" to result in a high risk to people's rights and freedoms, a DPIA is mandatory. Using biometric recognition systems usually triggers this requirement and even if special category biometric data is not used, the proposal to use biometric data may still be considered high risk. Specialist expertise may be required to analyse the specific risks in greater detail. Organisations should also consider whether the system used for biometric recognition involves privacy enhancing technologies (PETs) which can provide greater data protection.

It is important for organisations to be clear about the circumstances in which they act as a controller, including whether at any stage they might be a joint controller with another organisation. Any processors involved must only use biometric data when instructed by the controller. If processors act outside of instruction from a controller, they are using the data for their own purposes and may be subject to regulatory action unless they comply with the obligations on a controller. Any services outsourced by controllers should be regularly monitored to ensure compliance with data protection law and with applicable contractual terms.

Processing special category biometric data is often only permitted when explicit consent is provided by the individual to whom the data relates. However, an alternative must be offered to people who choose not to consent to the processing of their data so that they do not feel pressured to consent, which is particularly an issue for employers and public authorities. Suitable alternatives could include, for example, the use of a security PIN as an alternative to facial recognition systems to access restricted areas. Such alternative methods should be identified and explained in an organisation's DPIA to show compliance with data protection law.

Other conditions applying to biometric recognition

Explicit consent is likely to be the only valid condition for processing available to process special category biometric data. Other conditions may apply, but these will depend on the specifics of the proposal and the justification for using special category biometric data. In a limited number of circumstances, it is possible that an alternative condition under Article 9 of the GDPR can be relied upon if seeking explicit consent is not appropriate in the circumstances. These may include:

> “A risk analysis should be carried out to consider any potential circumstances which may threaten the security of the data, any damage which may be caused if such data is compromised, and what forms of attack systems may be subject to.”

I. **Prevention and detection of unlawful acts**

This condition applies where biometric data is required for the prevention of crime or detection purposes and it would not be appropriate to seek prior consent to the use of biometric data. It must be shown that the use of special category biometric data is necessary and targeted to deliver the particular specific purpose and for reasons of substantial public interest. An appropriate policy document must be put in place.

II. **Research**

Using special category biometric data for research purposes is permitted subject to being necessary for the research purposes and being a reasonable and proportionate way to achieve the purpose. Further safeguards must be complied with to ensure the use of the biometric data is safe, including demonstrating that the use of special category biometric data is:.

- not likely to cause someone substantial damage or substantial distress; and
- in the public interest.

For any condition for processing special category personal data to apply to the use of biometric recognition, it is important that all relevant requirements are met. If explicit consent has not been given and no alternative condition applies, it is unlawful to use biometric data as this would infringe data protection law.

Additional considerations

Biometric data presents inherent risks, and the processing of biometric data via a biometric recognition system should only be done with full consideration of alternative options and how the data may be compromised if protocol is not followed.

The ICO summarises the key risks as:

1. **Accuracy** – where the system generates errors because it does not correctly identify people;
2. **Discrimination** – where individuals or groups are treated unjustly on the ground of protected characteristics; and
3. **Security** – where unauthorised people can access the biometric data, or the system can be tricked (spoofed) into allowing access when it should not.

Biometric recognition systems use “probabilistic matching” to identify similar values in data, and use these similarities to make statistically informed guesses which the end user receives for their intended purposes. Organisations should be aware that these matching systems have the potential for errors including false positives and false negatives, and recognise that in certain contexts, other solutions may be more appropriate. The ICO also recognises that due to, for example, disability, some biometric recognition systems may be inherently biased, which may lead to discrimination. For instance, a person who is unable to use a fingerprint scanner due to a disability may be unable to access a specific device compared to a person who is able to use the biometric solution.

The security of biometric data must be thoroughly and appropriately considered by organisations processing it. A risk analysis should be carried out to consider any potential circumstances which may threaten the security of the data, any damage which may be caused if such data is compromised, and what forms of attack systems may be subject to. Any biometric data used must be encrypted and regular testing of the security system should be undertaken to ensure that protection measures remain effective over time.

For further information, please contact.

ANTHONY WOOLICH
Partner, London,
T +44 (0)20 7264 8033
E anthony.woolich@hfw.com

Assistance provided by Lucy Macris, Trainee Solicitor.

HFW has over 600 lawyers working in offices across the Americas, Europe, the Middle East and Asia Pacific. For further information about our EU, Competition and Regulatory capabilities, please visit hfw.com/EU-Competition-and-Regulatory.

© 2023 Holman Fenwick Willan LLP. All rights reserved. Ref: 005255

Whilst every care has been taken to ensure the accuracy of this information at the time of publication, the information is intended as guidance only.
It should not be considered as legal advice. Holman Fenwick Willan LLP is the Data Controller for any data that it holds about you.
To correct your personal details or change your mailing preferences please email hfwenquiries@hfw.com

Americas | Europe | Middle East | Asia Pacific