New ICO guidance on biometric data: the impact on e-signing platforms

September 2023

Richard Oliphant

The Information Commissioner's Office (**ICO**) has published guidance on biometric data and biometric technology. The guidance explains how UK data protection law (**UK GDPR**) applies to the use of biometric data in '*biometric recognition systems*'. It is aimed at organisations that use, and vendors that supply, biometric recognition systems, and applies to both controllers and processors.

The guidance covers:

- What constitutes biometric data
- When it is considered '*special category data'*
- The data protection requirements when biometric data is used in biometric recognition systems

ICO is consulting on the guidance. The consultation closes on 20 October 2023. ICO has signalled that it will issue a call for evidence early next year with a focus on biometric classification and data protection.

In this briefing, I assess the guidance and its impact on commercial e-signing platforms.

1. What is biometric data?

Art 4(14) of UK 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*."

The most common form of biometric data are physical or physiological characteristics such as a person's fingerprints, face, iris or voice which are used in '*biometric recognition*' (see section #3 below).

2. What is special category biometric data?

Biometric data falls within the definition of '*special category data'* if it is processed "*for the purpose of **uniquely identifying** a natural person.*"

Additional requirements apply to the processing of special category data. An organisation that wishes to process biometric data in the course of verifying identity will require the data subject's **explicit consent** (*Article 9, UK GDPR*).

3. What is biometric recognition?

ICO uses the term '*biometric recognition'* to describe the automated recognition of a person based on their biological (or behavioural) characteristics.[1] It encompasses both '*biometric identification'* and '*biometric verification'*.

Biometric identification asks the question: "*who is this person?*" The biometric data of one person in a biometric enrolment database is compared with that of many other people to find a match.

Biometric verification is slightly different. It refers to a 1:1 matching process. A person provides their biometric data for comparison with a stored biometric template (e.g. a facial image stored on a biometric passport). It asks the question: "*is this person who they claim to be?*"

Biometric recognition is now being used in a wide array of use cases. They include:

(a) **Mobile phone access**. A mobile phone can be unlocked with the user's own fingerprint or facial biometrics.

(b) **Airport security**. Airports leverage facial biometrics at security checkpoints. The passenger looks into a camera and AI compares the live photo with their passport photo.[2]

(c) **Remote customer onboarding**. Banks and other financial institutions rely on biometric recognition systems to remotely onboard their customers and satisfy their AML and KYC requirements.[3] The customer uploads a scan of their passport (or other photo ID document) and takes a video selfie. The system uses AI to match the facial biometrics in the passport and video selfie and confirm that they are of the same person.

(d) **Access control systems**. Fingerprint or facial biometrics may be deployed for granting access to the workplace or a gym as an alternative to a swipe card.

4. What are the data protection requirements when using biometric data in biometric recognition systems?

Any use of biometric data must be compliant with UK GDPR and other applicable data protection laws.

Requirements include:

(a) Data protection by design. You must adopt a '*data protection by design'* approach. The ICO guidance states that data protection and privacy must be considered from the outset and during the lifecycle of biometric recognition system. The user of a biometric system – for example, a bank deploying facial recognition technology to verify a customer's identity – should only work with vendors who provide "*sufficient guarantees of the measures they will use for data protection by design*."

(b) Data Protection Impact Assessment (DPIA). The use of a biometric recognition system will trigger a requirement for a DPIA. The DPIA should address the likelihood and potential impact of risks arising from the processing of biometric data, and measures to mitigate these risks. This will require technical assistance from the system vendor to ensure that the user understands the system and its capabilities.

[1] This aligns with the ISO/IEC biometric standard 2382-37:2022.
[2] Facial biometrics may also be used to board the plane in lieu of presenting a passport and boarding pass.
[3] In the UK, these requirements mainly derive from Regulation 28 of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 and Guidance produced by The Joint Money Laundering Steering Group.

(c) Identify the controller and processor. The user of a biometric recognition system should identify when they act as a controller or joint controller of biometric data. The system vendor is generally classed as a processor and should only use biometric data when instructed by the controller. But a system vendor frequently wishes to use the biometric data generated by users to develop and improve their system. In this case, the vendor is acting as a controller. The user of the system will have to notify any data subjects whose biometric data is processed by the vendor, and obtain their explicit consent.

(d) Explicit consent. Explicit consent is likely to be the only valid condition for processing special category biometric data under UK GDPR. If a data subject does not give their explicit consent, and there is no alternative Article 9 condition to rely on, the processing of special category biometric data would be unlawful. In this scenario, you must not use a biometric recognition system.

This is not a hypothetical risk. Last year, ICO fined the facial recognition database company, Clearview AI Inc more than £7.5m for, inter alia, failing to meet the higher data protection standards for collecting and processing special category biometric data. Be under no illusion: regulators are eager to clamp down on the abuse and misuse of biometric data.

(e) Accuracy risks. Biometric recognition systems use probabilistic matching to determine whether the captured biometric data (e.g. in a video selfie) is '*sufficiently similar*' to a stored biometric template (e.g the photo held on the chip in a biometric passport). A user of a biometric recognition system should consider the potential for false positive[4] and false negative[5] errors, and document this in their DPIA.

(f) Bias and discrimination. Users of a biometric recognition system must assess whether it is likely to have a discriminatory impact on people. Biometric technology uses AI and is susceptible to bias and discrimination. ICO cites data that shows fingerprint recognition is less accurate for adults over 70 and children under 12. This could be seen as *potentially* discriminatory. But there are workarounds such as offering a non-biometric authentication mechanism (e.g. password and PIN) alongside the biometric recognition system.

(g) Security. UK GDPR requires controllers to apply appropriate security measures to safeguard personal data. The likely damage caused by a breach or loss of biometric data[6] as well as the rising threat of attacks[7] against biometric recognition systems make security even more important. The user of the system should address security matters in the DPIA. For example, the DPIA should lay out the types of security threat posed to the system, testing, encryption, anti-spoofing and other security measures implemented by the system vendor.

5. Why is this relevant to e-signing platforms?

We are witnessing a nascent shift away from the traditional mass market model of electronic signatures and SMS authentication. The leading platforms are rapidly integrating with third party identity providers (**IDSPs**) and qualified trust service providers (**QTSPs**) on the EU Trusted List. IDSPs and QTSPs verify a signatory's identity to a higher level of assurance than SMS authentication. Identity fraud is on the increase in the UK banking and telecom sectors.[8] We are entering the new era of the '*verified identity*'.

[4] Also known as type I errors, false positive errors occur when a system incorrectly observes a case as positive when it shouldn't. In other words, a match is suggested, but the image does not match the person.
[5] Also known as type II errors, false negative errors occur when a system incorrectly observes a case as negative when it should be positive. In other words, the image does match the person, but the system did not recognise them.
[6] Issuing a new password is far easier than dealing with a situation in which a person's biometric data has been compromised.
[7] The NCSC has published guidance on the different types of attack on biometric recognition systems here.
[8] https://www.cifas.org.uk/newsroom/fraudscape23-release

Adobe Acrobat Sign has launched a new Digital Identity Gateway enabling its customers to choose from a wide range of IDSPs for identity verification, and complementing its ever-expanding roster of QTSPs who have integrated with the platform using the Cloud Signature Consortium technical standard. DocuSign has also augmented its identity verification capabilities with the introduction of DocuSign Identify and ID Verification.

This shift towards verified identities has coincided with the creation of the UK Digital Identity and Attributes Trust Framework (**DIATF**). The Department of Science, Innovation and Technology (**DSIT**) is overseeing beta testing and the DIATF is set to regulate how digital identities (and attributes) can be deployed in the UK as an alternative to physical forms of ID such as passports and bank statements. Digital identities will be used and reused for online transactions and interactions in the private sector (for example, to enable remote customer onboarding by banks and other FS institutions).

A significant number of the IDSPs that are certified against the DIATF have integrated with e-signing platforms. Digidentity and OneID have API integrations with Adobe Acrobat Sign. OneID and Onfido are integrated with DocuSign. E-signing platforms such as Yoti and VirtualSignature have gone one step further and certified themselves against the DIATF.

I predict a sharp rise in platforms offering verified identity solutions and a consequential decline in SMS authentication – particularly in regulated sectors like financial services, legal, telecommunications, real estate and healthcare – where IDSPs have an intrinsic role to play in AML and KYC ID checks.

However, e-signing platforms and their IDSPs will have to consider the ICO guidance in framing their verified identity solutions for customers. The guidance is also a reminder of the need to continually review and assess their general compliance with UK (and EU) GDPR:

- Many of the IDSPs offering a verified identity to a signatory are using biometric recognition systems and processing the signatory's biometric data. They may only do this with the signatory's explicit consent.

- These IDSPs are required to complete a DPIA under UK (and EU) GDPR. Where the IDSP is certified against the DIATF, this should not be a concern. The DIATF rules set a high bar for data protection, information security management[9], encryption and cryptography. Rule 15.13 of the DIATF lays out detailed, but non-exhaustive, data protection requirements which are largely based on UK GDPR. They include the need for explicit consent to process biometric data, privacy by design, data minimisation and **require** the IDSP to complete a DPIA. Further assurance is provided where – like Digidentity – the IDSP is also a certified QTSP under the EU eIDAS Regulation (No 910/2014).

- A customer relying on an IDSP that is not certified against the DIATF (nor an EU QTSP) must ensure they undertake thorough due diligence on that IDSP's compliance with applicable data protection laws, its security measures and obtain a copy of the IDSP's DPIA.

- If IDSPs are using a biometric recognition system, the ICO guidance suggests that their customers must also complete a DPIA. ICO notes that "*it is highly likely that you [customer] will trigger this requirement by using any biometric recognition system."* ICO also point out that where the use of a biometric recognition system involves several different organisations, they must be clear about who is acting as the controller, processor or, in some cases, joint controllers. This is never as straightforward as it seems.

[9] Certified IDSPs generally conform to ISO/IEC 27001. This is a standard for '*information security management systems'.*

- Where e-signing platforms are offering verified identity solutions to customers, they need to think carefully about the parties' roles under UK (and EU) GDPR. Who is the controller of the biometric data? Who is the processor? Who is storing the biometric data? Can the customer store or access the biometric data after a signatory has been verified? How is biometric recognition recorded in the platform's digital audit trail? The designated roles will depend on whether the platform is reselling the IDSP's services or facilitating a direct contract between the IDSP and the customer. A quick trawl of DocuSign's website illustrates how e-signing platforms need to raise their game. DocuSign has some impressive new verified identity solutions; but its GDPR analysis is too simplistic. It does not take account of the fact that some of their new IDSPs (e.g. Onfido) are processing signatories' biometric data let alone cover key requirements such as data protection by design or security measures.

- It should be acknowledged that whilst there is a strong trend towards the use of biometric recognition, some IDSPs offer non-biometric alternatives. The market-leader here is OneID. They are integrated with leading e-signing platforms and use Open Banking technology to verify the signatory's identity. There is no need for the signatory to produce a photo ID document nor take a selfie. Instead, the signatory logs into their online bank account and their bank leverages their KYC ID check to confirm the signatory's identity. There is no processing of biometric data and therefore no requirement for a customer (such as a bank or law firm) to complete a DPIA when using this verified identity solution.

If you would like to discuss this briefing or have questions about the ICO guidance on biometric data, you can reach me via email (richardoliphant@gmail.com) or via Linkedin.