Processing Biometric Data in the Workplace

Tim Hickman, Partner at White & Case LLP, advises on the practical implications of using biometric technologies in the workplace, and how to meet the requirements of the GDPR/ UK GDPR and EU AI Act

With their promise of greater security combined with less inconvenience, biometric technologies are increasingly being integrated into working environments. Fingerprint scanners and facial recognition are replacing swipe cards and PIN codes for securing physical access to sensitive areas; facial recognition is replacing passwords for accessing computers; telephone voice recognition systems are replacing lengthy sets of security questions; automated tracking technologies are even improving customer convenience by allowing in-person shopping without the need to interact with a cashier or present a payment card. As these technologies become more sophisticated and accessible, their presence in the workplace is set to grow even further.

While biometric technologies provide advantages that are undeniable for many organisations, they also pose potentially significant risks. One major concern is the potential for data breaches. Whereas a password can be reset if it has been compromised, biometric data cannot. In addition, biometric recognition systems are not always accurate, and can suffer from both false positives and false negatives. Like any security technology, the protection offered by biometric systems is not infallible. Further, the processing of biometric data can have a substantial impact on the privacy of employees, customers and visitors.

There are laws that are designed to help address these risks, including the GDPR/UK GDPR and the EU AI Act. Processing biometric data in compliance with these laws presents a number of challenges, however. It should be noted that the EU AI Act specifically states that it does not affect the GDPR, which means that organisations will typically be required to comply with both regimes in parallel.

Biometric data and the GDPR/UK GDPR

As well as attracting the usual compliance obligations imposed by the GDPR/UK GDPR regarding any processing of personal data, biometric data is a form of 'special category data', and is therefore subject to stricter requirements. In particular, the legal bases available to an organisation that wishes to process biometric data are limited (as set out in Article 9(2) GDPR/UK GDPR). For most organisations, the only realistically available legal basis for processing biometric data in a workplace context is getting the explicit consent of affected data subjects (Article 9(2)(a) GDPR/UK GDPR).

In addition to being explicit, such consent must take the form of a freely given, specific, informed and unambiguous indication of the data subject's wishes (Article 4(12) GDPR/UK GDPR). However, in a workplace context, it can be very difficult to show that consent has been 'freely given', due to the imbalance that often exists between an employer and an employee. As the European Data Protection Board has explained in paragraph 21 of its Guidelines 05/2020, "it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal." There are, of course, situations in which an employer could obtain freely given consent from employees, but these are limited to scenarios in which the employee is genuinely free to refuse, without any fear of penalties or adverse consequences.

Therefore, when implementing biometric security in the workplace, organisations need to find a way to provide the affected employees with a genuine choice regarding the processing of biometric data.

Taking the example of biometric access to a secure workplace, an organisation could allow its employees the choice of two different ways to gain secure entry:

- use of a standard biometric security system (e.g., security gates that operate on the basis of facial recognition); and
- use of a more traditional system (e.g., security gates that use a

(Continued on page 4)

(Continued from page 3)

combination of a swipe card and a PIN).

On the basis of the following, the employer has a good argument that those employees have validly given explicit consent to the processing of their biometric data.

- the employer provides the employees with clear information concerning the nature and purposes of the processing that will take place in each case;
- employees are free to select whichever option they prefer; and
- the employer obtains (and keeps a record of) consent from those employees who select the biometric option.

Guidance from the UK Information Commissioner's Office on biometric data provides a similar example regarding access to a gym. Importantly, it must be possible for employees who have consented to the processing of their biometric data to withdraw that consent at any time (Article 7(3) GDPR/UK GDPR). In the above example, this would mean that the employer would need to allow such employees to switch to the swipe card and a PIN option.

Beyond the requirement to obtain explicit consent, organisations need to ensure that they comply with the standard 'background' GDPR/UK GDPR compliance requirements when processing special category data of employees (e.g., implementing appropriate security measures, data protection by design and by default, data transfer measures, purpose limitation, maintaining records of processing, giving effect to the rights of employees, etc.). Most importantly, the processing of biometric data in a workplace context may trigger the requirement to complete a data protection impact assessment ('DPIA') (Article 35(3)(b) GDPR/UK GDPR) and consultation with the organisation's Data Protection Officer, if it has one. Any such DPIA will need to be kept under review, and updated as the biometric processing technology evolves over time.

Biometric data and the EU AI Act

The EU AI Act introduces a sophisticated framework for regulating biometric technologies, with multiple definitions and categories. The EU AI Act also has a very aggressive extraterritorial scope (see '*The EU Act Part 2*', Volume 24, Issue 6, pages 13-14) meaning that it is often likely to apply to organisations in the UK, and elsewhere outside the EU, even where those organisations are not operating in the EU.

The EU AI Act uses the same definition of 'biometric data' as the GDPR, but adds definitions of (among others):

- 'biometric identification' (i.e., automated recognition of individuals based on biometric data);
- 'biometric verification' (i.e., automated one-to-one verification of a person's identity by comparing their biometric data against a record) although this term is only used once in an operative provision;
- 'biometric categorisation systems' (i.e., systems that assign individuals to specific categories on the basis of their biometric data); and
- 'remote biometric identification systems' (i.e., systems that identify individuals without their active involvement).

This complexity can make it difficult for organisations to understand and comply with the specific requirements for each type of biometric technology.

Most implementations of biometric technology in the workplace are likely to fall within the EU AI Act's very broad definition of an 'AI System' (see '*The EU Act Part 1*', Volume 24, Issue 5, paragraph 14-15). AI Systems that are used for the purposes of remote biometric identification, biometric categorisation, or emotion recognition, are categorised as 'high-risk' under Annex III of the EU AI Act. High-risk AI Systems are subject to stringent compliance requirements, including transparency, assessments, documentation, governance, and human oversight obligations. (Note that some of the assessment requirements can be met by completing a DPIA, as referred to above).

However, AI Systems that process biometric data for the limited purpose of confirming that a specific individual is the person he or she claims to be are not categorised as 'high-risk'. This means that most biometric security systems in the workplace are likely to be categorised as 'limited risk' and will therefore attract fewer compliance obligations under the EU AI Act.

Conclusion

Due to the sensitive nature of biometric data and the stringent requirements imposed by the GDPR/UK GDPR and the EU AI Act law, the use of biometric technologies presents several challenges. Organisations need to navigate these challenges with care, by ensuring that they have appropriate consent mechanisms and other GDPR/UK GDPR compliance measures in place, and by ensuring that they understand which of their AI Systems are likely to be categorised as 'high-risk' or 'limited risk' under the EU AI Act and implementing the corresponding compliance measures. This requires each organisation to gather enough information to have a clear understanding of how each biometric technology will function in practice, in order to determine which compliance obligations apply in each case. As the regulatory environment continues to evolve, organisations will need to stay informed and adapt their compliance structures to meet these requirements.

Tim Hickman
White & Case LLP
tim.hickman@whitecase.com