What GDPR means for Biometrics

It's just been a matter of weeks since the General Data Protection Regulation (GDPR) was introduced. While there is no single over-arching piece of legislation that covers the collection and use of biometric data, there are a number of different laws that cover the area of privacy around biometrics, including the GDPR. As Emma Butler, Data Protection Officer for Yoti explains, "In the UK there is no specific biometric legislation but biometric data used to identify an individual is classed as 'sensitive data' under data protection law. This means it is subject to particular rules and safeguards and its use is more restricted. In addition, the US has specific biometric legislation in several states". David Cook, Solicitor Advocate at Eversheds Sutherland adds, "What we have is a patchwork of different laws that go some way in covering the area in relation to the holding and use of this material by the state, by employers and by commercial organisations." These laws include:

- Data protection law in the form of elements of the General Data Protection Regulation and the Data Protection Act 2018
- Human rights laws with respect to the right to private life under Article 8 of the European Convention on Human Rights and Schedule 1 of the Human Rights Act 1998
- Oversight on the use of biometrics by the government, through the Commissioner for the Retention and Use of Biometric Material, a role that they are obliged to fill by Section 20 of the Protection of Freedoms Act 2012

The newly introduced GDPR covers the use of personal data by organisations and "sets out quite onerous obligations around what they do with personal data, with a sub-category of personal data which has additional safeguards, says David.

"The main impact is the change in classification from 'ordinary data' to 'sensitive data', says Emma. "This means that in certain circumstances the lawful basis an organisation used before 25 May now needs to be supplemented by an additional lawful basis for sensitive data. In the UK, national law has retained the fraud prevention lawful basis for processing sensitive data, which is often the purpose of biometric data processing. However, this does not exist in other EU countries' national law, making it more difficult for organisations wanting to operate across the EU. GDPR allows for Member States to introduce additional lawful bases for sensitive data, but so far, to my knowledge, only the Netherlands and Croatia have done this for biometric data.

"Many organisations may now need to use explicit consent as their lawful basis instead and so need to provide for that consent to be withdrawn, as well as the additional rights attached to using consent as a lawful basis. Where organisations offer online services to children that involve biometrics (children are defined differently in different Member States) and they use consent as their lawful basis, they will need to age gate and get parental consent.

"In addition, there is a particular difficulty for employers using biometric access controls for increased security reasons, given consent in this employment context would not be considered valid.

"Finally, organisations collecting and using biometric data on a large scale will now be legally obliged to carry out a privacy impact assessment."

David continues, "The GDPR sets out very stringent requirements on organisations to demonstrate why they need to process biometric data. The ongoing compliance with the GDPR after that point is also an issue: a breach of the GDPR in relation to biometric data will be seen as a significant breach. The Information Commissioner's Office (ICO) has previously stated that a security breach around sensitive data affecting even a single data subject could be considered serious enough to warrant a monetary penalty."

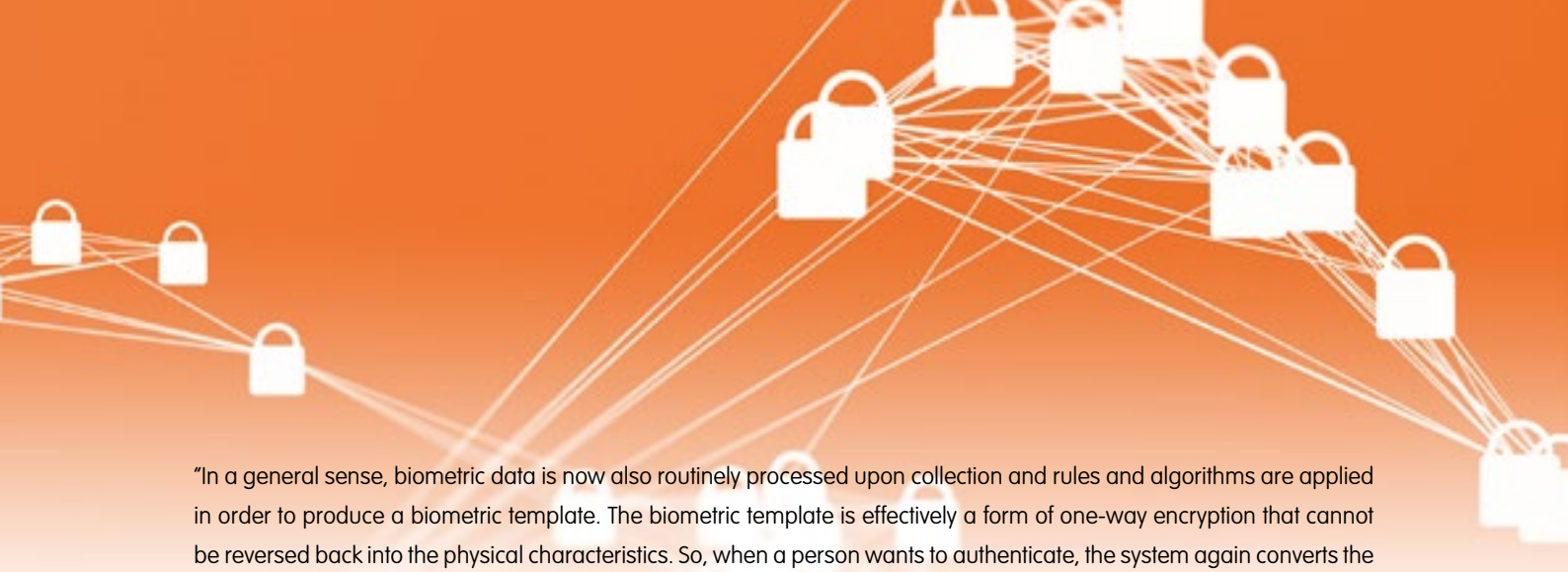
So, what should an organisation be considering when it collects and uses biometric data? In Emma's opinion the same basic considerations apply to any proposed collection and use of personal information: "Why you are collecting it; what you will do with it; where you will store it; who will have access; and how you will secure it. It becomes more important with sensitive data like biometrics to have suitable security and access controls and to consider if your collection and use is ethical, fair, proportionate and justifiable. The lawful basis you use will also dictate other obligations and requirements."

The processing conditions set out with respect to the GDPR demonstrate the scale of the task. An organisation considering the use of biometric techniques also needs to consider the GDPR principle of Data Protection by Design and by Default. "The use of new technology like biometric techniques, on a large scale and using automated processing, leads to an obligation to undertake a Data Protection Impact Assessment (DPIA)" says David. "If the DPIA established that the proposed use of biometrics presented a high risk to the rights and freedoms of individuals, then the organisation should consult with the regulator before proceeding. In certain circumstances, the organisation should also consult with the individuals likely to be affected. These are seriously rigorous safeguards to ensure that the use of biometric data is only ever carried out in limited circumstances and, even then, with the risk to those affected kept absolutely minimal."

Making sure that biometric data isn't stolen or re-used is critical so it's important to have the right technology controls in place. According to David, fairly sophisticated security approaches are being deployed to meet this need. "A good example is the iPhone which routinely deploys fingerprint scanning technology to authenticate the user. The use of the biometric data is limited to authentication protocol and no more. Biometric data is stored within the Apple Secure Enclave security chip on the phone and is not stored on Apple servers or via the iCloud.

David Cook
Solicitor Advocate
Eversheds Sutherland

Emma Butler
DPO
Yoti



"In a general sense, biometric data is now also routinely processed upon collection and rules and algorithms are applied in order to produce a biometric template. The biometric template is effectively a form of one-way encryption that cannot be reversed back into the physical characteristics. So, when a person wants to authenticate, the system again converts the biometric characteristics by this process and it is the conversion data that is compared against the template. The biometric characteristics are not stored; just the template.

"This process is broadly similar to how systems authenticate passwords: a user types in their plain text password, which is processed by a security algorithm and might be hashed and salted and it is the product of that process that is compared against what is stored – the plain text password is not stored and the risk to individuals is minimal if the stored password 'template' is lost.

"Having said that, there will be circumstances in which biometric data is lost by organisations. In order to prevent it from being re-used to allow access to information and devices that should not be allowed, we are now seeing the increased use of multi-factor and multi-modal authentication: the biometric data is not the only data to be provided and the person must still use another form of verification in order to authenticate."

Using Artificial Intelligence (AI) alongside biometric data is another key area for consideration. Emma says "There are certain countermeasures to prevent exposure of private information when training on sensitive biometric data. Privacy-preserving machine learning is a research line that focuses on developing countermeasures against attacks which try to reverse engineer a trained machine learning model. These countermeasures can be roughly categorised into two groups: those that work to prevent the model relying too much on the data of any specific individual during training; and those that deliberately add noise to the training data."

In David's opinion, the combination of artificial intelligence and biometric data is one that might be expected to be high risk and therefore something for which the regulator must be consulted about. "The GDPR sets out that a DPIA should be carried out for the use of new technology and the ICO has issued guidelines that state that it expects a formal assessment for the use of artificial intelligence." Explaining this further, David says "The GDPR seeks to cover the use of behavioural characteristics such as biometric data and the determination and definition of those characteristics by an artificial intelligence platform is a prospect that most people would find alarming. The GDPR sets out to tumble such an idea through a set of cogs and mechanisms and deliver a compliant product at the end of it through the organisation: processing only in specific and limited circumstances, being transparent around what is proposed; implementing Data Protection by Design and by Default; completing a DPIA and consulting with the regulator and data subjects as necessary and, complying with the onerous terms of the GDPR regarding sensitive data."

It's not clear yet how this all works in practice however David is certain that 'novel and new technological advances are going to occur and are going to test the terms of the GDPR. What data subjects find acceptable will also shift over time. It's clear however that the GDPR enforcement regime can be unforgiving and organisations that want to conduct such practices will need to be squeaky clean from a data protection or privacy perspective in order to manage the commercial risk."