

Europe's tough new law on biometrics

Sam De Silva and Anthony Liu, Nabarro LLP

As the adoption of biometric technologies becomes more widespread, the security issues involved are getting more important – how and where should biometric data be stored and secured, and how is the data being used and processed? The EU's new General Data Protection Regulation (GDPR) addresses some of these concerns by introducing controls and provisions that every organisation using or intending to use biometric authentication needs to be aware of.

So what is the GDPR and to whom does it apply? The regulation is the EU's new data protection law, first proposed by the European Commission in January 2012. It was approved by the European Parliament in April 2016 and will come into force in just over a year's time, on 25 May 2018, after a two-year transition period. The GDPR will apply across all EU member countries, without them needing to implement their own national legislation. The advantage of this is that it should, in theory, establish more uniformity in how data protection law is applied and enforced across Europe. When the GDPR takes effect, it will replace the EU's existing data protection legislation (the Data Protection Directive), as well as all individual national legislation on data protection, such as the UK's Data Protection Act (DPA).

In essence, the GDPR embodies the same core data protection principles as the Directive, while building on them by strengthening individuals' rights; paying more attention to cyber-security and technological capacity; and tightening up supervision and sanctions. The law applies to all data controllers and processors – broadly speaking, a controller says how and why personal data is processed, and the processor acts on behalf of the controller. The GDPR is applicable to organisations that are established in the EU, offer goods and/or services in the EU and/or monitor the behaviour of EU citizens. A significant change introduced by the GDPR is the accountability of processors. This extends the personal data protection responsibility to all companies involved in the handling of data, such as cloud service providers.

Biometric data

The existing EU Directive already had the concept of 'special categories' of 'sensitive personal data', but the GDPR expands on this to expressly include 'genetic data' and 'biometric data' that is processed 'to uniquely identify a person'. Classifying biometric data as sensitive

personal data effectively means such data needs to be treated separately and gives it a higher level of protection.

The new law's special categories of sensitive data now include: data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; data concerning health, sex life and sexual orientation; genetic data; and biometric data where processed to uniquely identify a person. Biometric data under the GDPR is defined as any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or 'dactyloscopic' data.

Article 9 of the GDPR sets out the circumstances in which the processing of sensitive personal data – which is otherwise prohibited – may be allowed (this is discussed in more detail below). Recital 51 of the GDPR notes that the processing of photographs will not automatically be considered as sensitive processing. Photographs will only be covered to the extent that they allow the unique identification or authentication of an individual as a biometric, such as when it is used as part of an electronic passport.



GDPR tightens the rules on handling biometric data for organisations who are based in or offer goods or services in the EU, and/or who monitor the behaviour of EU citizens.



Sam De Silva

Processing sensitive data

The grounds for processing sensitive data under the GDPR broadly replicate those under the Directive and the UK's DPA, but have become slightly narrower. Organisations that currently process sensitive data should be clear about what conditions they rely on to process such data, and check whether those conditions are still applicable under the GDPR. As with the current Directive, the processing of sensitive data is subject to more stringent conditions than other forms of personal data. Any processing of personal data must satisfy at least one of the following conditions:

- Explicit consent from the data subject, unless reliance on consent is prohibited by EU or member state law. This condition is equivalent to the wording in the DPA.
- Necessary for the carrying out of obligations under employment, social security or social protection law, or a collective agreement. This condition expands on the wording in the DPA by making reference to compliance with employment obligations or obligations under social security, social protection law and collective agreements.
- Necessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent. This condition is equivalent to the wording in the DPA.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim, provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent. This condition is equivalent to the wording in the DPA.
- Data manifestly made public by the data subject. This condition is equivalent to the wording in the DPA.
- Necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity. This condition is equivalent to the wording in the DPA, but there is additional wording relating to the processing of data by courts acting in their judicial capacity.

- Necessary for reasons of substantial public interest on the basis of EU or member state law, which is proportionate to the aim pursued and which contains appropriate safeguarding measures. This condition, in essence, means that member countries can extend the circumstances in which sensitive data may be processed in the public interest.
- Necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services, on the basis of EU or member state law or a contract with a health professional; and necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health-care and of medicinal products or medical devices. These two conditions expand on the position under the DPA by providing legal justification for regulatory uses of health data in healthcare and sharing health data with providers of social care.
- Necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1). This is a new condition introduced by the GDPR, which allows for the processing of sensitive data for the purposes of archiving, research and statistics.



Organisations processing significant amounts of biometric data should beware that individual EU countries can put their own extra controls on the use of genetic, biometric or health data.

which the UK formally withdraws from the European Union (Brexit), has meant that the UK Government has had to review the impact of the GDPR. Until Britain formally leaves the EU, the Directive and DPA are still applicable. The current view is that the formal process triggering Brexit, which could last two years, will be invoked some time during 2017. This means the UK would be part of the European Union until 2019 at the latest. So when the GDPR comes into force, it will be relevant for many organisations in the UK, particularly for those operating internationally.

Baroness Neville-Rolfe, the UK's Minister for Data Protection, has confirmed that if the UK remains within the European single market, EU rules on personal data might continue to apply fully in the UK. But in other scenarios, all EU rules might be replaced with national ones. Current thinking suggests that the UK Government intends to negotiate a national-level data privacy solution, rather than leave UK organisations to rely on individual bilateral arrangements, such as EU-approved contract clauses or specific exemptions for data exports.

On that basis, there are some practical steps that UK organisations who use biometric technology, and who have customers in the EU, should consider. First, they should create a map of their organisation's personal data flows with EU countries and consider where such data resides. They should also ask themselves the following questions in relation to data flows:

- To what extent do you use EU or 'third country'-based service providers to process your data (for example, payroll processing, back office, IT infrastructure)?
- Are adjustments likely to be needed to ensure that data can continue to flow post-Brexit?
- Where does the legal responsibility fall in relation to making such adjustments?
- Would it be feasible to enter into EU model contracts to enable such data flows to continue? Alternatively, could the servicing of those relationships be switched to an alternative EU group company (bearing in mind other possible consequences, such as tax and resourcing)?
- Are there higher-risk data types involved in some of these data flows (for example, health data, human resources data, bank account data)?

- What additional provisions can be made to ensure the continuity of those data flows?

Key strategic questions

Whether UK-based or not, all organisations affected by the GDPR need to consider the following key questions:

- Is your organisation a controller or a processor?
- Is the data you process 'ordinary' personal data or 'sensitive' data (or both)?
- Is your organisation within the territorial reach of the GDPR?
- Can you rely on consent or other lawful grounds to process data?
- What is your data export strategy, is it appropriate and how does this impact your wider compliance model?
- Is there any profiling, monitoring or tracking activity to consider?

Simple guidance

The UK Information Commissioner's Office (ICO) has published a helpful 12-step guide to assist organisations in preparing for the GDPR. The key points – which also largely apply to companies outside the UK – are summarised here (some have already been covered):

1. **Awareness.** Ensure that key decision makers are aware of the law changing to the GDPR, the likely impact of that change, particularly in areas likely to cause compliance problems, and the resource implications for achieving compliance.
2. **Information audit.** Organisations are advised to document the personal data held across the organisation and within particular departments, where the data originated from, and with whom the data is shared.
3. **Communication.** Organisations should review privacy notices in light of anticipated GDPR changes. These changes include the requirement to explain in a short, simple and clear manner the legal basis for processing data, data retention periods and the right to complain to national regulators.
4. **Individuals' rights.** Procedures should be checked to ensure they cover how to properly manage a request from an individual seeking to exercise their GDPR rights. In the UK, these rights are mainly the same as under the DPA, but additional GDPR rights arise around preventing profiling and a new right to data portability.
5. **Subject access requests.** Organisations should update their policies and procedures to handle new GDPR features in relation to subject access requests. These should cover a one-month time limit to respond and the need to provide data subjects with extra information, for example on data retention periods and their right to have inaccurate data corrected.

Country differences

Under Article 9(4), EU member states are entitled to maintain or impose further conditions (including limitations) relating to genetic, biometric or health data. That being the case, existing country differences in the approach on these topics are likely to be maintained, and there is scope for further divergence. So organisations that process significant amounts of biometric data should be wary of individual member states imposing additional conditions, as set out in the GDPR.

One example of a difference in national approach has already been seen in France. In September 2016 the CNIL, the French data protection authority, announced that it had adopted two new authorisations, which will replace the previous biometric decisions and set out the CNIL's position on biometric systems used to control access to workplace premises, and/or software applications and devices in the workplace.

UK, Brexit and the GDPR

The result of the UK's June 2016 referendum on EU membership, and the process by

6. Legal basis for processing personal data.

The ICO's guidance suggests that organisations should examine the types of data processing they carry out. They should document the legal basis for carrying out each type of processing (in the UK broadly the same as those in the DPA), which will also assist with meeting GDPR accountability requirements. They should also set out the legal basis for processing in terms of privacy notices and when responding to subject access requests.

7. Consent. The GDPR contains additional measures around consent. 'Consent' or 'explicit consent' must be freely given, specific, informed and unambiguous. Consent must also be a positive indication of agreement to data processing – it cannot be inferred from silence, pre-ticked boxes or inactivity. It must be verifiable. Therefore, the ICO recommends that organisations should review how consent is sought, obtained and recorded. Secondly, they should consider whether alterations or alternatives to consent mechanisms are necessary to meet the GDPR requirements and to provide an audit trail for demonstrating consent.

8. Children. The GDPR provides special protection for children's personal data, especially in the context of commercial internet services, such as social networking. It also allows each EU member country to determine what they consider the age of the child to be (between 13 and 16). In the case of the UK, the ICO indicates that it is likely to legislate to provide for anyone under 13 to be a child, and so recommends that organisations should consider systems to use for verifying individuals' ages and to obtain parental or guardian consent, which the GDPR will require to lawfully process a child's data. Organisations that aim their services at children should also note that privacy notices must be written in language that children will understand.

9. Data breaches. As mentioned above, the GDPR will introduce a general duty to notify national bodies of certain types of breaches. This differs from the DPA where only certain types of organisations must report breaches by law. The ICO's guidance suggests organisations should ensure procedures are in place to detect, report and investigate a personal data breach and they should document the types of personal data held which would fall within a notification requirement.

10. Data protection by design and data protection impact assessments. The ICO's guidance suggests that organisations do the following: adopt a privacy by design and data minimisation approach to all activities involving data processing; become familiar with guidance on Privacy Impact Assessments (PIAs); assess situations where it will be necessary to conduct a PIA; and determine who will conduct the PIA, who needs to be involved and whether it should be run centrally or locally.

11. Data protection officers. Under the GDPR, a new obligation arises to appoint a data protection officer (DPO) in certain cases – for public authorities or organisations whose activities involve regular and systematic monitoring of data subjects on a large scale. Organisations should:

- Designate a DPO, if required. Otherwise, assign responsibility for data protection compliance to a particular person or role (internal or external).
- Ensure the DPO or person responsible is appropriately qualified, effectively supported and has appropriate authority within the organisation.
- Decide where the DPO or person responsible will fit within the organisation's governance structure.

12. International control. A new GDPR one-stop shop system will change the way complaints involving processing across multiple

member states are assigned among data protection supervisory authorities.

Act now or pay later?

Finally, the GDPR introduces substantial fines for data privacy violations. National data protection authorities will be able to impose fines of up to 4% of total worldwide annual turnover or €20m (whichever is higher). For less serious violations, the data protection authorities will be able to impose fines of up to 2% of total worldwide annual turnover or €10m.

So while the GDPR will not come into force until the spring of 2018, organisations should start their preparation now by reviewing their current data collection practices and examining the new requirements. Organisations that have already introduced appropriate measures to ensure compliance with the GDPR are unlikely to undo this preparation, as compliance will make it easier for them to conduct their activities in the EU. But those organisations who fail to meet GDPR standards may find it more challenging to work with clients in the EU once the GDPR is implemented.

About the authors

Dr Sam De Silva is a partner at Nabarro LLP and regularly advises on data protection, privacy and cyber-security issues. He is the UK representative on both the EU Commission's Expert Group on Cloud Computing Contracts and the IT Law Committee of the Bars and Law Societies of Europe. Sam is also on the Privacy & Policy Expert Group of the Biometrics Institute. Anthony Liu is a qualified lawyer at Nabarro LLP in the Intellectual Property and Information Technology team. He specialises in e-commerce, technology commercial contracts, cyber-security and data protection and privacy.

The future of identity verification

Robert Capps, NuData Security

When the idea of networked computing was first developed, security really was the last thing on programmers' minds. Then, when it became clear that it was desirable to lock away some sensitive information, a basic username and password system was developed. But now as we move more and more critical business online, the risks and attacks mounted against such a decrepit and inadequate system are apparent. As an industry, we have responded by bolting on a hodge-podge of workarounds designed to provide identity verification, including active and passive biometrics. But the reality is we've just added more complexity...without adding effective security. What we need is less chewing gum and duct-tape security, and a whole lot more imagination and innovation to revolutionise online user authentication.



Robert Capps

The inherent weaknesses in the static username and password system – passwords repeated across multiple websites and poor security on many sites – have led to the current arms race with hackers. As security technologists get better at protecting the keys to a user's online identity, the hackers must get better at finding them. The race goes on because it's a game of