COSMOS
Navigate the Compliance Universe

CEP Magazine - March 2018
It's not too late to comply with GDPR!

By Robert Bond

Robert Bond (robert.bond@bristows.com) is Partner & Notary Public at Bristows LLP in London, United Kingdom.

The EU General Data Protection Regulation (GDPR) comes into force on 25 May 2018, and it will have a significant impact upon Legal and Compliance.

Because GDPR is a regulation, it will be instantly binding on each EU member state from 25 May 2018 whether or not those member states have implemented variations to their local data protection laws.

Many member states are already making changes to their data protection laws to mirror GDPR, and since they have certain derogations that allow them to make local changes, we will be faced with the need to review each member state's approach to certain aspects of GDPR.

Applicability

What is certain is that GDPR will apply to controllers and processors that have subsidiaries or affiliates in the EU. A controller is a business that makes decisions in relation to personal data, whereas a processor is a third party that carries out processing on behalf of the controller.

GDPR has an extra territorial nature in that it applies to any controller or processor that is not located in the EU but has processing activities related to either the offering of goods or services to data subjects in the EU, irrespective of whether a payment is required or not — or where the processing activities relate to the monitoring of the behaviour of EU citizens so far as that behaviour takes place within the EU.

Many businesses will be caught by GDPR whether or not they have entities in the EU. If controllers or processors outside the EU are caught by GDPR, and if they process large volumes of sensitive data, or if such processing could result in a risk to the rights and freedoms of individuals, then they will have to designate in writing a representative who must be established in a member state where the data subjects whose data are being processed are located. When processing of EU citizens' personal data takes place in several member states, the representative will need to be appointed in the member state where most of the EU citizens are located whose data is being processed.

The role of the representative is to sit between the controller or processor and the relevant supervisory authority and/or data subjects. The representative will need to respond to investigations or communications from the relevant supervisory authority and/or from data subjects and need to have in place a suitable contract to define roles and responsibilities. The designation of a representative does not affect the primary responsibility and liability of the controller or processor under GDPR.

Data protection principles

GDPR lays out eight data protection principles, which are similar to those under current law. These principles are that personal data must be:

- Processed fairly, lawfully, and in a transparent manner;
- Collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those;
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which personal data is processed;
- Accurate and, where necessary, kept up to date;
- Kept in the form which permits identification of data subjects for no longer than is necessary;
- In accordance with data subjects rights;
- In a way that ensures appropriate security of the personal data;
- Not transferred to a third country or to an international organisation if the provisions of GDPR are not complied with.