DATA PROTECTION

THE **NEW EU REGIME** AND WHAT IT MEANS FOR THE ISLE OF MAN

The European Union is introducing new regulations governing data protection. **Claire Milne**, a partner within the Corporate Department at Appleby, examines the potential implications for the Isle of Man.

The current data protection regime in the European Union (EU) dates back 20 years – before the growth of the internet and the digital economy. The European Commission put forward its data protection reforms in January 2012 to make, in its view, the EU fit for the digital age. After much debate, the new reforms have now been accepted. The main reform is the General Data Protection Regulation (GDPR). As the new regime will be effected by way of regulation (rather than directive) it will have direct effect in each EU member state and therefore, each member state will have exactly the same legislation. The Isle of Man is not part of the EU but has adopted legislation that is modelled on current EU data protection legislation to allow the Isle of Man to obtain a so-called "adequacy finding." An adequacy finding means that the European Commission has deemed that the Island's law ensures an adequate level of protection for personal data and this aids the transfer of personal data in and out of the Island. To retain its adequacy finding, the Isle of Man will need to enact new data protection legislation following the changes to the EU regime.

GDPR – NEW RIGHTS FOR INDIVIDUALS

- easier access to data – an individual will have more information as to how his data is processed and this information should be available in a clear and understandable way;
- a right to data portability - it will be easier to transfer your own personal data between service providers;
- a clarified "right to be forgotten" - when an individual no longer wants his data to be processed and provided that there are no legitimate grounds for retaining it, the data will be deleted.

GDPR - NEW RULES FOR BUSINESSES

- businesses with establishments in various EU member states will benefit from the so-called "one-stop-shop" principle. This means that the supervisory authority of the main establishment of a processor or controller is competent to act as "lead supervisory authority";
- businesses based outside of the EU will have to apply the EU data protection rules when offering goods or services in the EU;
- no more notifications to data protection regulatory authorities;
- data processors will have direct obligations;
- personal data breaches must be notified to the competent supervisory authority within 72 hours, where feasible. Breaches that are unlikely to result in a risk to the rights and freedoms of data subjects do not need to be notified;
- certain organisations will be required to appoint a data protection officer;
- stricter requirements regarding the giving of "consent" for processing of personal data;
- privacy by design and privacy impact assessments mean that privacy issues will need to be considered at the outset of any new project or activity, rather than as an afterthought;
- power to issue fines of up to 4% worldwide annual turnover for breaches.

The new rules will become applicable in two years but action needs to be taken now to ensure your business has sufficient time to comply. While some of the provisions (such as stopping the requirement to notify) will ease some administrative burden, others will mean a significant change is required in relation to data protection compliance and will require all organisations to review their internal policies and procedures in relation to the collection and processing of personal data. Data protection issues will require to be considered as part of an overall compliance regime and therefore will be an issue for a company's Board to consider.