information commissioner
Barrantagh Fysseree

The EU General Data Protection Regulation (GDPR) entered into force on 24 May 2016. There is a two year transition period before the GDPR becomes fully enforceable on 25 May 2018.

The GDPR is "Text with EEA Relevance," which means it applies to all European Economic Area (EEA) countries, which comprises the 28 EU member states and Iceland, Liechtenstein and Norway.

The GDPR is extraterritorial in scope and applies to businesses outside the EU that process the personal data of EU residents or process personal data on behalf of an EU data controller.

Failure to comply with the GDPR could lead to a fine of up to €20 million or 4% of annual turnover. There will be further effective and persuasive penalties for Directors and officers. EU Data Protection Authorities have also been provided with powers to ban processing and suspend the transfer of personal data to a third country.

GDPR & BREXIT

The UK Government has confirmed that the GDPR will be implemented in the UK as required by 25 May 2018.

The Secretary of State Karen Bradley MP recently appeared before the Culture, Media and Sports Select Committee and confirmed:-

"*We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public.*"

This statement also confirms that the GDPR will apply to businesses outside the UK that process the personal data of UK residents or process personal data on behalf of a UK data controller.

The UK Information Commissioner's recent keynote speech at the National Association of Data Protection and Freedom of Information Officers Annual Conference on 21 November emphasised her intention, in respect of Brexit, to *"be at the centre of any conversations, and will be banging our drum for continued protection for consumers, clear laws for organisations, and all the usual aspects that we'll need to continue trading with Europe."*

GDPR & Isle of Man businesses

Isle of Man businesses that offer goods or services to UK or EU residents, or process personal data on behalf of a UK or EU business, must comply with the provisions of the GDPR by 25 May 2018.

Such businesses need to prepare for the GDPR and can expect to be asked to demonstrate how they comply with the requirements of the GDPR by any UK/EU data controller with whom they do business. An inability to do so could result in that UK/EU data controller deciding to terminate business rather than risk the fines and sanctions that could be imposed upon it.

After 25 May 2018, businesses that offer goods or services to UK/EU residents will also be subject to supervision by an EU data protection authority. Businesses should expect be required to demonstrate how they comply with the requirements for the GDPR to the UK or another EU data protection authority. Failure could result in a substantial fine and the authority could impose a ban on the transfer of personal data to that business.

Is the Isle of Man implementing the GDPR?

In June, Council of Minsters considered the implications of GDPR. The Summary of Proceedings states:

> *"Council considered a paper submitted by the Cabinet Office and approved the policy statement which would provide businesses with a commitment that the Isle of Man Government intends to adopt the General Data Protection Regulations by mid-2018."*

Since then there has been a General Election and a new administration in the Isle of Man. During the debate on the "Programme for Government" in Tynwald, on 15th November 2016, the Chief Minister confirmed:-

> *"On 14th April this year, the European Union approved the new General Data Protection Regulations (GDPR) … Therefore, we must ensure that we continue to operate to the standards and practices expected of us in this area. We are committed to retaining our existing adequacy rulings in relation to data protection. We will take whatever steps are necessary in the future to ensure adequacy in relation to the GDPR."*

The Isle of Man has an existing adequacy finding under the current European Directive which permits personal data to be transferred to and from the EU. This finding will continue to apply when the GDPR comes into force but could be removed at any time and must be reviewed within four years, i.e. by 2020.

However, both the European Data Protection Supervisor (EDPS) and the Article 29 Committee, which comprises all 28 EU data protection authorities, have stated that current adequacy findings do not meet the requirements of the GDPR. It is clear that they expect businesses located outside the EU that process the personal data of EU residents to meet the requirements of the GDPR.

To retain an adequacy finding the Isle of Man must introduce "essentially equivalent" legislation to the GDPR. Although no time frame for doing so was provided in the Chief Minister's statement, equivalent legislation will be implemented in the near future.

It may be worth noting that both Jersey and Guernsey have committed to introducing equivalent legislation by May 2018.

Council of Europe Convention 108

Council of Europe Convention 108 is the original European data protection instrument and was extended to the Isle of Man in 1993.

Brexit does not affect the UK's membership of the Council of Europe and therefore its Conventions, including the European Convention on Human Rights and Convention 108, will continue to apply.

Convention 108 is in the process of being modernised and final agreement is anticipated by the end of January 2017. The modernised version is expected to contain high level provisions similar to those detailed in the GDPR.

In the event that Brexit results in the UK leaving not only the EU but also the EEA, any future UK data protection law would still need to meet the provisions of the modernised Convention 108.

European Data Protection Board

The GDPR created the European Data Protection Board (EDPB) comprising the EDPS and the 28 data protection authorities of the EU. The EDPB is responsible for providing guidance on how to interpret the GDPR.

EDPB guidance - proposed schedule
The EDPB intends to have the first tranche of guidance finalised by the end of 2016. Those publications are likely to address the role of the Data Protection Officer, the new right of data portability, and how to identify an organisation's main establishment and lead supervisory authority.

Guidance on the concept of risk and conducting a Data Protection Impact Assessment is already being worked on, with an estimated completion date of February 2017. Work has also commenced on guidance on certification.

The EDPB guidance will be published on the Commissioner's website as and when it becomes available.

UK ICO Publications

The UK ICO advice on GDPR can now be found at: https://ico.org.uk/for-organisations/data-protection-reform/

In addition to the previously published "Overview of the GDPR" and the "12 Steps to Take", the UK ICO has published a new Code of Practice,

"Privacy Notices, transparency and control". This can be found at: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

The Code of Practice takes into account the Transparency requirements of the GDPR, an area of significant change from current data protection legislation. In particular, the Code of Practice gives Isle of Man businesses, which provide goods or services to UK residents, a clear explanation on how compliance with the Transparency requirements of the GDPR can be achieved.

The UK ICO intends to publish further guidance on consent and profiling by the end of January 2017.

Training opportunities

Whilst the Information Commissioner is happy to attend events to raise awareness of the GDPR, due to the size of the office and the additional responsibilities for Freedom of Information, the Information Commissioner will not be running CPD training events.

Publications available

The website contains various publications in the section "Steps towards compliance". These include:

"The GDPR Game Changers" - An awareness-raising presentation

"The GDPR – Steps towards compliance" - An overview of the GDPR

"Know your data: Mapping the 5 W's" – GDPR Toolkit Part 1

"Accountability - A questionnaire for senior management" – GDPR Toolkit Part 2

Previous issues of the GDPR newsletters are also available and an RSS feed is available for all news items published on the website.

Get in touch

If you have questions about the GDPR, or would like to make comments about the content of any of our publications, please contact us.