Introduction to the new Isle of Man data protection law

information commissioner
Barrantagh Fysseree

How the new data protection law works
The Act, Orders and Implementing Regulations described below, together with any further Orders and Regulations subsequently made, are collectively referred to as 'the data protection law'.

Data Protection Act 2018
The Data Protection Act 2018 permitted the EU General Data Protection Regulation (GDPR) and EU Law Enforcement Directive (LED) to be applied to the Island by 'Order' and brought into effect through 'Implementing Regulations'.

Two Orders have been approved by Tynwald in accordance with the Data Protection Act 2018: - the Data Protection (Application of the GDPR) Order 2018 (SD2018/0143) and the Data Protection (Application of the LED) Order 2018 (SD2018/0144). Other Regulations and Orders can be made.

There are no compliance provisions contained in the Data Protection Act 2018.

Data Protection (Application of the GDPR) Order 2018
This Order is of relevance to the private and public sector.

The text of the EU GDPR is included in the Annex to the Order. The EU GDPR text contains Island amendments and strikeouts prescribed in the main body of the Order and the annexed EU GDPR text, as adapted, is called the **"Applied GDPR"**. The Applied GDPR is the main body of the data protection law in the Island with which controllers and processors must comply.

The **Applied GDPR** does not include matters such as exemptions and restrictions, criminal sanctions, registration etc.. These matters are set out in the Implementing Regulations. The Implementing Regulations are subordinate to the Applied GDPR and must be read with the Data Protection (Application of the GDPR) Order 2018. Where there is any conflict, the Applied GDPR takes preference.

The **Implementing Regulations** effectively contain the nuts and bolts that hold the superstructure of the Applied GDPR together.

The compliance obligations under the EU GDPR and the Applied GDPR are substantially similar and businesses engaged in markets including residents in the EU therefore have one generalised set of rules to follow. Such businesses should, however, be aware that they may be subject to regulation by a data protection supervisory authority in an EU Member State and make themselves aware of any national laws in their EU markets that contain provisions on exemptions, sanctions etc. akin to those in the Isle of Man's Implementing Regulations.

Data Protection (Application of the LED) Order 2018
The public sector, and private sector organisations (if any) which provide probation or youth justice services on behalf of a government department, or have contractual responsibility for securing electronic monitoring, parole or bail conditions of a natural person, must also comply with another Order, the Data Protection (Application of the LED) Order 2018, and the associated relevant regulations in the Implementing Regulations.

Those public and any relevant private sector bodies are known as "competent authorities".

The 'LED Order' and associated Implementing Regulations only apply to specific personal data processed for prescribed purposes by competent authorities – i.e. personal data only being processed for the purposes of the prevention, investigation, detection or prosecution of **criminal offences** or the execution of **criminal penalties**, including the safeguarding against and the prevention of threats to public security, by that competent authority. This document does not include any further guidance on the LED Order.

The GDPR and LED Implementing Regulations SD2018/0145

The following is a summary of the parts of the **Implementing Regulations** that impact on the functional operation of private and public sector businesses and organisations (including charities, voluntary organisations, sports clubs etc.). The provisions marked with an asterisk **(*)** are those most immediately relevant to the private sector.

Part 1 (Regs 1 – 8)

Basic legal information and a few definitions

Part 2 * (Regs 9 – 25**)**

Provisions explaining why the law looks like it does and provisions dealing with:

- child's age of consent for information society services,
- public interest condition for processing,
- exceptions to the prohibition on processing special categories of personal data and criminal convictions etc data,
- additional matters regarding rights of data subjects.

Regs 19-21 are about FOI and only impact public sector

Regs 22-25 are about national security (public sector) and a power to make further exemptions.

Parts 3, 4 & 5 (Regs 26 – 75 except Regs 62, 68, 69 & 75) and Schedule 12

Applied LED provisions which ONLY apply to "competent authorities" listed in Schedule 1

Except:

- Reg 62 – just says articles 37-39 of the Applied GDPR apply to DPOs appointed under the Applied GDPR
- Regs 68/69/75***** – international transfers under Applied GDPR – see also Schedule 10

Part 6 (Regs 76 – 100) and Schedule 3

Additional provisions about the Commissioner's functions, powers and obligations

Part 7* (Regs 101 – 134) read with Schedules 4, 5 & 8

Provisions about enforcement, appeals, compensation, offences (some are recordable offences/carry 6 months in prison)

One of the main differences is in **Reg 114** - the maximum penalty that can be imposed by the Commissioner is **£1M** in the context of an infringement of the Applied GDPR by controllers and processors established or processing in the IOM (see Reg 8 for application of the Implementing Regulations)

Part 8 (Regs 135 – 150)

Technical provisions but include a ban on asking individuals to make access requests for personal data in some circumstances (read with Schedule 6 & 8) and Directors' etc. liability

Schedules (if not mentioned above)

Schedule 2 * – **conditions for processing special categories of personal data and criminal convictions data lawfully** – you will need to digest this. Note Part 4 of this schedule which mandates certain information to be recorded in records of processing maintained under Article 30 of the Applied GDPR.

Schedule 7 * – **registration** – this includes changes in the exemptions from registration. The new registration regime has effect from 1 August 2018 for brand new registrations and from February 2019 for renewals (which will be deemed as new registrations for the purposes of the new data protection law). Articles 5 and 6 of the Data Protection (Application of the GDPR) Order 2018 have effect together with Schedule 11 of the Implementing Regulations and the Data Protection (Fees) Regulations 2018 (SD 2018/0169).

Schedule 9 * – **restrictions and exemptions** – important, but long and a bit complicated, so read carefully.

Schedule 11 * – **transitional arrangements** – note in particular that:

- If you are relying on the consent of individuals as the lawful ground for processing their personal data (not for electronic direct marketing as that is under the Unsolicited Communications Regulations) you have until 25 May 2019 to make sure that the consent accords with the Applied GDPR provisions.
- You must get your transparency information (privacy notices etc.) updated to meet the new requirements of the Applied GDPR and provided to data subjects by 25 May 2019.
- If you have an existing subject access request that has not been finalised by 31 July 2018, it will be treated as if it was an access request made under the Applied GDPR from 1 August 2018.