information commissioner
Barrantagh Fysseree

Final GDPR newsletter

The new data protection law came into effect in the Isle of Man on 1 August 2018 after the GDPR and LED Implementing Regulations 2018 were approved by Tynwald in the July sitting.

The law constitutes the following:

- Data Protection Act 2018
- Data Protection (Application of GDPR) Order 2018 (SD2018/0143)
- Data Protection (Application of LED) Order 2018 (SD2018/0144)
- GDPR and LED Implementing Regulations 2018 (SD2018/0145)
- Data Protection (Fees) Regulations 2018 (SD2018/0169)

All these instruments, including the secondary legislation, can be found via Isle of Man Government's legislation portal https://www.legislation.gov.im/cms/index.php

Some changes to the Implementing Regulations are expected to be laid before Tynwald this Autumn. In addition, a Bill, to replace the "Information Commissioner" with a statutory board, together with consequential provisions, is anticipated in early 2019. It is likely that the Bill proposals will be subject to a Cabinet Office consultation.

These changes are, however, unlikely to impact on the fundamental operation of the law as far as controllers and processors are concerned, with the Data Protection (Application of GDPR) Order 2018, and incorporated Applied GDPR, remaining in place.

This final "GDPR Newsletter" summarises the main compliance requirements of the law approved by Tynwald in July 2018.

GET IN TOUCH

If you have questions, or would like to make comments about the content of any of our publications, please contact us. You can also keep up to date by following us on LinkedIn https://www.linkedin.com/company/isleofmaninformationcommissioner

Compliance requirements of the new law

In summary, the compliance requirements are:

Principles of data protection

The principles whilst similar to those of the Data Protection Act 2002, do include some changes and enhancements which are in bold for ease of reference. Note that the rights of individuals and the rules concerning international transfers of personal data are no longer listed as 'principles'.

The principles can be found in Article 5 of the Applied GDPR and are:

- Lawfulness, fairness and transparency
  - Fair processing information must be **"provided"** to data subjects
- Purpose limitation
  - Processed for "specified, **explicit** and legitimate purposes"
- Data minimisation
  - "Adequate, relevant and **limited to what is necessary** in relation to the purposes for which they are processed"
- Accuracy
  - Where personal data is inaccurate they should be "**erased or rectified without delay"**
- Storage limitation
- Integrity and confidentiality (this can be referred to as the security principle)
  - Use of appropriate technical and organisational measures to ensure appropriate security (security of processing is further defined in Article 32)

See the dedicated section of the website: https://www.inforights.im/information-centre/data-protection-law-2018/principles-of-data-protection/

Article 5(2) brings the principles together and requires controllers to be responsible for, and be able to demonstrate compliance with the principles. This is referred to as "**accountability"**.

See the dedicated section on the website: https://www.inforights.im/information-centre/data-protection-law-2018/accountability-and-governance/accountability/

Mandatory personal data breach reporting by controllers

All personal data breaches must be recorded by controllers. (Applied GDPR, Article 33(5))

Personal data breaches that pose any risk to the rights and freedoms of individuals must be reported to the Commissioner. (Applied GDPR, Article 33(1))

If there is high risk to the rights and freedoms of individuals the controller must notify the individuals concerned. (Applied GDPR, Article 34)

See the dedicated section on the website, including the reporting form, at: https://www.inforights.im/information-centre/data-protection-law-2018/personal-data-breach/

Data Protection Officers

Data protection officers must be appointed by controllers and processors if required and the Commissioner must be notified of the person appointed. (Applied GDPR, Article 37(7))

See the dedicated section on the website, including the reporting form, at: https://www.inforights.im/information-centre/data-protection-law-2018/data-protection-officers/

Registration

Controllers and processors must, unless exempt from the requirement, be registered with the Commissioner. (Regulation 9, Implementing Regulations)

There are changes to the exemptions from the requirement to register, specifically that the processing of personal data for the purposes of direct marketing is no longer classed as an exempt core business purpose and registration will be required if personal data is processed for such direct marketing (e.g. email/sms marketing).

There are also changes to the process for registration and for those controllers with existing register entries that expire before 1 February 2019, there are transitional arrangements.

See the dedicated section of the website for more information about registration, including the relevant application forms, at: https://www.inforights.im/information-centre/data-protection-law-2018/registration/

Records of processing activity

It is a mandatory requirement in some cases for controllers or processors to maintain records of processing activities. (Applied GDPR, Article 30)

The details of processing are no longer recorded by the Commissioner as part of registration and even where mandatory records are not required, some form of record detailing the processing being undertaken is recommended as they can, amongst other things, assist controllers and processors to demonstrate accountability for their processing, provide the basis for transparency information to individuals, and inform security measures.

See the dedicated section of the website at: https://www.inforights.im/information-centre/data-protection-law-2018/accountability-and-governance/records-of-processing-activities/

Compliance with rights

Individuals have some new and enhanced rights under the new law and the timescale for complying with rights is one calendar month. In addition, no fees can generally be levied. (Applied GDPR, Articles 12-22)

See the dedicated section on the website at: https://www.inforights.im/information-centre/data-protection-law-2018/rights/

Complaints to the Commissioner

Individuals can make complaints to the Commissioner regarding any infringement of the data protection law, including failure to comply with their rights. (Regulation 122, Implementing Regulations)

The Commissioner has various powers available to him to handle such complaints. (Regulation 77, Implementing Regulations and Applied GDPR, Article 58(1))

See the dedicated section on the website at: https://www.inforights.im/complaint-handling/how-to-make-a-complaint-to-the-information-commissioner/data-protection-complaints-2018/

Offences, sanctions and penalties

There are several offences under the new law which are dealt with through the court and the Commissioner also has a suite of sanctions available to him for infringements of the law. (Regulation 77, Implementing Regulations and Applied GDPR, Article 58(2))

This includes the power to impose a financial penalty of up to a maximum amount of £1,000,000. (Regulation 114, Implementing Regulations)

See the dedicated section on the website at: https://www.inforights.im/information-centre/data-protection-law-2018/offences-sanctions-and-penalities/

Cooperation with the Commissioner

Controllers and processors must co-operate with the Commissioner in the exercise of his tasks, whether that is related to handling a complaint or otherwise, and failure may result in the imposition of a financial penalty. (Applied GDPR, Article 31)

More information on the new data protection law is available on the website and is gradually being updated as time and resource permits.

Other resources

Links to the following can now be found on the website:

- Council of Europe - Convention 108
- The European Data Protection Board (EDPB)
- EDPB Guidelines, Recommendations, Best Practices
- EU Member State Data Protection Authorities
- The EU Commission
- UK Information Commissioner's Office
- Ireland Data Protection Commission's Office
- Guernsey Data Protection Commissioner
- Jersey Information Commissioner

See: https://www.inforights.im/information-centre/data-protection-law-2018/links/