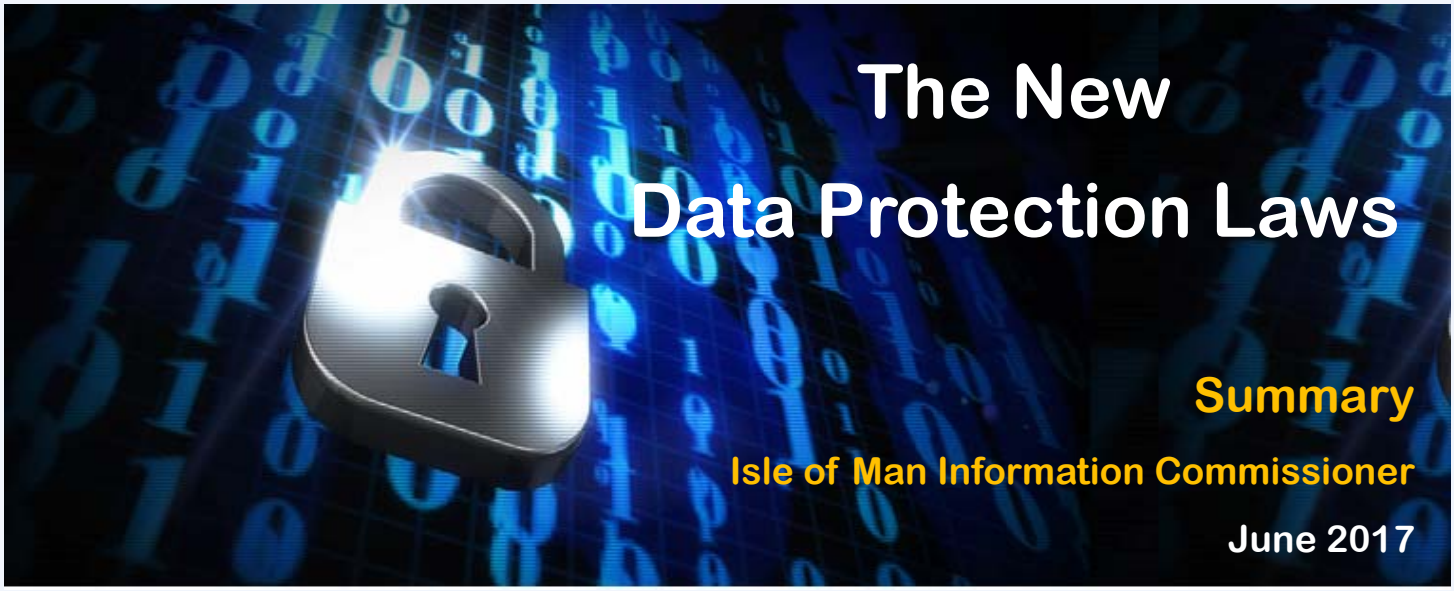

The New Data Protection Laws

Summary

Isle of Man Information Commissioner

June 2017

Data is now an important commodity in the global economy. Current data protection laws are outdated and do not afford individuals sufficient rights and protection against the risks associated with modern ubiquitous processing. International bodies including the OECD, APEC, Council of Europe and the EU have recognised these risks. and responded by creating new rules. The EUs response, has resulted in several new data protection instruments including the General Data Protection Regulation (GDPR).

The GDPR seeks to strengthen the protection of personal data by making good data protection practice and governance an integral part of business and a boardroom responsibility. It provides individuals with new, stronger rights and protections and also provides supervisory authorities with new powers including the ability to audit, suspend or ban processing and impose financial penalties up to 4% of global turnover.

The GDPR takes a risk based approach. Organisations that can demonstrate good data governance practices can expect customer trust and confidence, while those that fail to do so can expect penalties and loss of business.

The territorial scope of the GDPR means that it applies to any Isle of Man company providing goods or services to EU residents.

To continue to provide the highest standards of protection and maintain its "adequacy finding" the Island intends to introduce essentially equivalent legislation. In the Programme for Government recently approved by Tynwald, the Chief Minister has taken responsibility to do so.

The intention is to implement equivalent legislation by 25 May 2018.

Awareness

The new laws place the onus upon an organisation to demonstrate compliance. Awareness needs to be raised throughout the organisation with boardroom and senior management team support essential.

Organisations need to review current processing to establish what it needs to do to achieve compliance and identify the human, financial and technical resources needed to do so.

Effectively dealing with new obligations including data breach reporting and enhanced rights, such as the improved right of access and the right to object to processing, requires planning.

With less than 12 months to go the amount of time and effort required should not be underestimated.

At a Glance

Accountability
onus upon data controller to demonstrate compliance

Transparency
using clear plain language

Data Security
regularly tested and certified

New Consent Rules

Data Protection Officers

Data Breach Reporting

New & Stronger Rights
free to exercise

New Supervisory Powers
Penalties up to 4% of turnover

Accountability

An organisation that determines the purposes and means of processing is known as *a 'controller'*. **A controller is responsible for compliance and must be able to demonstrate:-** (1) compliance with the principles, (2) appropriate technical and organisational data security measures are in place that are effective and regularly tested, and (3) that appropriate data protection policies have been implemented.

In determining what is appropriate the controller must take into account the nature, scope, context and purposes of processing as well as the varying likelihood and severity of risk to the rights and freedoms of the individual. Assessment of risk is therefore inherent to accountability.

A thorough analysis of current processing should occur with existing policies and procedures assessed to identify whether they are effective, adhered to, and whether changes are necessary to comply with the new laws.

RESOURCE

Accountability questionnaire for the Board Compliance Resources page at www.inforights.im

Getting Ready for GDPR — UK Information Commissioner

https://ico.org.uk/for-organisations/improve-your-practices/data-protection-self-assessment/getting-ready-for-the-gdpr/

Know your data

Every organisation must know what personal data it processes and understand the risk that processing may pose to the individual.

Knowing why, and when the processing occurs, whose data is processed, what data is processed, how it is obtained, where it is stored and for how long, whether it is transferred to any other organisation and if so why and where to, and what security measures are in place to protect that data are all essential for compliance with the new laws.

RESOURCE

Know Your Data: Mapping the 5 Ws at Compliance Resources page at www.inforights.im

Principles

Current processing needs to be reviewed against the revised principles. In summary these are:-

Personal data shall be

- Processed lawfully, fairly and in a transparent manner in relation to the data subject; **('lawfulness, fairness and transparency')**
- Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes…; **('purpose limitation')**
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; **('data minimisation')**
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, …, are erased or rectified without delay; **('accuracy')**
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed…; **('storage limitation')**
- Processed in a manner that ensures appropriate security of the personal data including protection against unlawful processing and against accidental loss, destruction or damage, using appropriate technical or or-ganisational measures. **('integrity and confidentiality')**

Transparency

Transparency is a new obligation and right intended to ensure that an individual understands what will happen to their personal data. It is a considerable change from the current fair processing requirements and therefore **likely to require resource and effort to achieve compliance.**

When a controller collects information from an individual, or indirectly obtains information about an individual, transparency requires that controller to provide information to the individual about the intended processing in a concise, transparent and easily accessible form using clear and plain language. This information includes:- the identify and contact details of the controller, and the controller's representative in the EU where applicable, the contact details of the Data Protection Officer where applicable, the purposes and legal basis for processing, any recipients of that data, any international transfers of the data and the measures in place to safeguard that data, how long the data will be stored, the rights of the individual, including access, rectification, objection and portability, the right to complain to a supervisory authority and, where processing is based on consent, the right to withdraw consent.

RESOURCE

Privacy Notices Code of Practice — UK Information Commissioner

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

Data Security

The responsibility to implement appropriate technical and organisational security measures include as appropriate:-

- The pseudonymisation and encryption of personal data;
- The ability to ensure ongoing confidentiality, integrity , availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Where it can demonstrate compliance with these requirements adherence to codes of conduct or other certifications schemes is encouraged

RESOURCE

A Practical Guide to IT security — UK Information Commissioner

https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

Consent

Where processing is based upon consent, the controller must be able to demonstrate that consent was freely given.

The method of obtaining consent must use clear plain language, be easily accessible and clearly distinguished from other matters. Consent will NOT otherwise be valid.

Consent may be withdrawn at any time and this must be explained when consent is sought. It must be as easy to withdraw consent as it was to give.

RESOURCE

DRAFT GDPR Consent guidance — UK Information Commissioner

https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

Data Protection Officer

A controller and processor must designate a Data Protection Officer (DPO) when processing is carried out either by a public authority, the core processing activities require regular and systematic monitoring of data subjects on a large scale, or, the core processing activities include large scale processing of certain special categories of data including, for example, data about health, racial or ethnic origin, political opinions and criminal offences.

Inter alia a DPO:-

- must be involved in all issues relating to the protection of personal data, should inform and advise of obligations, monitor compliance and be the contact point for data subjects and the supervisory authority;
- be provided with the resources necessary to carry out those tasks;
- must not be instructed, dismissed or penalised for exercising the tasks or have any other conflicting duties,
- must report directly to the highest level of management.

A DPO should have expert knowledge but can be a shared resource and does not have to be a member of staff.

RESOURCE

Guidelines on Data Protection Officers ('DPOs') : Art 29 Data Protection Working Party

http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_annex_en_40856.pdf

Data Breach Reporting

Where a personal data breach occurs, a controller must, without delay and where feasible within 72 hours of becoming aware of the breach, notify the supervisory authority unless that breach is unlikely to result in a risk to an individual.

A controller must describe the nature of the breach including the number of data subjects involved and records compromised, provide the contact details of the DPO or other contact point, describe the likely consequences of the breach, and describe the measures taken to address the breach including measures to mitigate any adverse effects.

Where the breach is likely to result in high risk to an individual, the controller must, without delay, also advise each data subject in clear and plain language of the nature of the breach and the measures taken to address and mitigate the breach. The exceptions to this requirement are when the data is protected, for example, by encryption, the high risk is no longer likely, or individual notification would be disproportionate and instead a public announcement for example would be more effective.

Rights

Existing rights have been strengthened and new rights created. Each right has specific requirements but in general these rights are free to exercise and a controller must comply promptly and within one month. These rights are:-

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure ***(Right to be forgotten)***
- Right to restrict processing
- Right to object to processing
- Right to data portability
- Right to prevent automated individual decision making and profiling

The purpose of this summary is to assist controllers to understand some of the new obligations. It is not definitive nor does it constitute legal advice.

information commissioner
Barrantagh Fysseree