The GDPR places much more emphasis on building an effective data protection practice and safeguards from the very beginning of all processing.

- Data protection must be considered early on in projects involving data
- Data Protection Impact Assessments (DPIAs) are best practice and likely to be mandatory in some circumstances such as
  - Decisions that produce legal effects
  - Processing of special category data e.g. health data
- Monitoring of publicly accessible areas

Ensure such processes become routine and well documented. As business models and processes change and evolve, so too do compliance needs. Regular reviews are therefore essential and should be proactively managed and recorded.

What, Where, Why, How

A detailed understanding of your own data processing underpins the accountability aspect of the GDPR. Any effective data governance strategy must be proactively managed and recorded. Regular reviews are therefore essential and should be proactively managed and recorded.

Penalties and Data Breaches

The GDPR provides for a tougher enforcement approach by the Data Protection Authority including the ability to impose significant fines.

- Data breaches must be notified to the Data Protection Authority within 72 hours of discovery.
- Individuals impacted should be told where there exists a high risk to their rights and freedoms e.g. identity theft, personal safety
- Fines can be issued up to €20 million or 4% of global annual turnover
- Data Protection Authority can issue reprimands, warnings and bar as well as fines

The level of fine is likely to depend on a number of factors including:

- Nature, gravity and duration including categories of data
- Intentional or negligent
- Action taken to mitigate damage
- Security and Privacy by Design measures
- Degree of co-operation
- How Data Protection Authority found out
- Previous enforcement activity
- Other aggravating or mitigating factors

It is essential for data protection to be integrated into corporate risk management for your organisation. Consider how you will manage breach reporting both internally and in respect of your obligations to the Data Protection Authority. If you use a data processor, be clear about your expectations in respect of breach management and ensure these expectations are incorporated into the relevant contracts.

Conclusion

There is no doubt that we are on the verge of huge change in data regulation. With the Channel Islands now committed to implementing the GDPR locally, it is vital for all organisations to understand the changes and to start to prepare for compliance. During 2017 we will see clarity about what the local legislation will look like as the law drafting work progresses. We will also start producing information and guidance during this time which will be available on our website www.dataci.org

The current data protection legislation – Data Protection (Bailiwick of Guernsey) Law, 2001 and the Data Protection (Jersey) Law 2005 (the current Laws) – were drafted in response to EU Directive 95/46/EC (the Directive) and declared adequate for the purposes of data transfers. The EU has recently approved the General Data Protection Regulation (GDPR), the largest change to the protection of personal data since the Directive in 1995. The GDPR comes into effect for EU Member States on 25 May 2018.

We are undoubtedly at a turning point for data protection and the GDPR has implications for the Channel Islands in two ways:

- Local companies targeting goods or services to EU citizens will be required to comply with the GDPR, regardless of what regulatory or legislative regime is in place locally.
- The Islands’ ‘adequacy’ ruling under the current EU Directive will be re-assessed against the GDPR and it is highly unlikely that the current Laws will be considered adequate against the new standard.

Both Governments have therefore made the decision that the GDPR will be incorporated into local law, with the aim to be ready for implementation in May 2018 in line with the EU legislative timetable.

Key Features

What some aspects of the current Laws are replicated in the GDPR, for example the processing condition (for the most part), the following are the key differences:

- Risk based approach to identification and increased documentary evidence required
- Accountability for data controllers and processors.
- Strengthened rights for individuals.
- Children afforded higher levels of protection.
- Mandatory breach reporting.
- Legitimate interests processing condition removed for public authorities.
Preparing for the GDPR

The following are ten areas that the Data Protection Commissioner has highlighted as significant matters to be aware of and the steps you can take to begin preparation for the new regulatory regime. Whilst aspects of the GDPR are new, many of the requirements build upon the existing legislative framework and therefore compliance with the current Laws will go a long way towards compliance with the GDPR.

Do not underestimate the time required to ensure you are fully prepared for 2018. The value of formulating, adopting and implementing exemplary data governance and security practices lies in the rewards it yields.

Key Features

Whilst some aspects of the current Laws are replicated in the GDPR, for example the principles and processing conditions (for the most part), the following are the key differences:

- Risk based approach to governance and increased documentary evidence required.
- Accountability for data controllers and processors.
- Strengthened rights for individuals.
- Children afforded higher levels of protection.
- Mandatory breach reporting.
- Legitimate interests processing condition removed for public authorities.

AWARENESS

As an organisation you must ensure you are aware of the changes ahead. You have the following:

- Chair-Based and Senior Management Team support. This is no longer an area that can be the responsibility of one individual. Board level engagement is essential.
- Consider the resource and procedural implications of putting in place robust and effective data governance for your organisation.
- Privacy and data security are now part of corporate risk management. Add GDPR to your organisation’s risk register.
- Teach key people with keeping up to date with data with developments and make sure they are at an appropriate level of seniority and adequately resourced.
- Two awareness sessions to ensure all staff are aware and up-to-date with the changes GDPR will bring to the organisation.

WIDER SCOPE

The GDPR will impact new and far reaching areas both geographically and procedurally. Many organisations will be captured by the requirements and more data processing will be encompassed by the definitions.

- Data Controllers come under the remit of the GDPR and will have specific compliance obligations.
- Organisations outside the EU, including Channel Island based companies, targeting EU citizens by offering goods or services or monitoring their behaviour will need to comply with the GDPR.
- If you have an EU presence or process data on EU citizens, you must comply with the GDPR.

CONSENT

The GDPR considers consent an important part of ensuring individuals have control and understanding of how their data are to be processed.

- Consent must be:
  - Freely given
  - Specific
  - Informed
  - Unambiguous
- There has to be a positive indication of agreement.
- Consent as a basis for processing gives individuals stronger rights.
- Data controllers must be able to evidence consent was given.
- Parental consent to process children’s data on the internet.

INDIVIDUAL’S RIGHTS

Individual’s rights are enhanced and extended in a number of important areas.

- A right of access to data (Subject Access).
- A right to the correction of data where inaccuracies have been identified.
- A right to the erasure of personal data (often referred to as the ‘right to be forgotten’).
- A right to prevent direct marketing.
- Control over automated decision making & profiling.
- A right to a data portability between controllers.

SUBJECT ACCESS REQUESTS (SARs)

As the GDPR captures more information within the definition of personal data, organisations will face increased demand for access requests. Your records management systems and processes, both document and paper-based, must be consciously designed to support the efficient deployment of information retention and retrieval.

- In most circumstances no fee can be charged.
- A response must be provided within 1 month.
- More information is required to be provided including data retention periods & rights to have data deleted.
- Policies & procedures will need to be in place to govern inquiring requests.

PRIVACY NOTICES

Empowering individuals by being transparent and clear about how their data are going to be processed and why is at a key element of compliance with the GDPR. At every point at which personal data are collected, shared, held or held by your clients, staff or others, review how you intend to provide the following at all times of collection:

- Purpose of and legal basis for processing;
- Recipients of the data;
- Any third countries data are transferred to and safeguards in place;
- Data retention periods;
- The existence of individual’s rights;
- Right to withdrawal consent where provided;
- Data Protection Officer’s contact details; 
- Whether data provision has statutory or contractual basis;
- Details where the legitimate interest condition has been applied.

DATA PROTECTION OFFICERS (DPOs)

Getting ready for the GDPR requires multi-disciplinary skills and approach. Identifying and supporting a member of your staff with responsibility for data protection compliance may be a mandatory requirement for your organisation. But even if it is not, having someone in place undertaking that role will be beneficial to your organisation.

The DPO role will require a solid understanding of the way your organisation operates and a skills set that stretches well beyond an understanding of legal compliance. It must include IT, data security, strategy, communication, risk management etc.

The GDPR is clear that such a role should be appropriately senior and autonomous. They will be expected to be the front face of data protection for your organisation which will necessarily include dealing with data subjects and the Data Protection Authority.

- DPOs likely to be mandatory for:
  - Public authorities.
  - Organisations involved in high risk processing.
  - Organisations processing special categories of data.

- DPO must be suitably experienced and skilled.
- Has set tasks including:
  - Inform & advise organisation of obligations.
  - Monitor compliance including awareness raising, staff training, audits.
  - Cooperate with Data Protection Authority and set as contact point.

- Can be shared with other organisations or have other functions too but none that conflict.

NOTES:

- The content is not legal advice.
- The content is subject to change without notice.
- The content is not intended to reflect all the requirements of the GDPR.
- The content is not intended to reflect the guidance of the Information Commissioner’s Office (ICO).
- The content is intended as a guide.
- The content is not intended to reflect the final version of the GDPR.
- The content is not intended to reflect all the requirements of the GDPR.
- The content is not intended to reflect the guidance of the Information Commissioner’s Office (ICO).
- The content is intended as a guide.
- The content is not intended to reflect the final version of the GDPR.