information commissioner
Barrantagh Fysseree

The General Data Protection Regulation

Steps towards compliance

March 2016

"Despite over four years of high profile negotiations … companies are still unaware and there is a worrying chasm between those who are actively preparing and those that are blind to the changes ahead"

Chris Babel CEO TRUSTe

Understand the new era of compliance

The GDPR brings fundamental changes to the data protection compliance regime and is ***"the biggest thing to happen in the privacy arena in 20 years".***
(Lisa Sotto, Hunton & Williams).

The GDPR is extra-territorial in scope and will directly apply to Island businesses and those ***"operating in Europe or targeting European customers need to get their act together and start preparing for the new regime."*** (Eduardo Ustaran, Hogan Lovells LLP)

Boards and senior management teams will be held accountable and the ***"new law gives directors 20 million reasons"*** to comply. (Christopher Graham, UK Information Commissioner)

Failure to comply may result in a European data protection authority imposing a fine of up to €20m or 4% global turnover and individual Directors or senior managers may also be prosecuted for non-compliance.

The ***"level of risk … has catapulted data protection into the boardroom".*** (Jane Finlayson-Brown, Allen & Overy)

Island businesses have two years to wake up to the new era of data protection compliance and get measures in place.

The main points are:

- Documenting and evidencing compliance
- Making and maintaining records of processing
- Stricter security requirements
- Stricter rules on transparency and data retention
- Data minimisation
- Explicit rules on 'consent'
- New rules for children's data
- New rules for processors
- Mandatory data breach reporting
- Restrictions on profiling

Action points:

- Inform colleagues
- Obtain boardroom support, including allocation of
    - Staffing
    - Funding
    - Requisite skills/knowledge
- Identify a leader/team; and
- Determine an approach to compliance

Know Your Data - Map the 5 W's

The GDPR will *"force companies to scrutinise how they process and handle customer data"* (Tony Pepper, Egress Software Technologies)

The requirements of enhanced fair and transparent processing, robust information security, records of processing activities and extended, stronger, rights require an in-depth knowledge of what personal data is processed and why.

Data protection is *"an afterthought no longer"* (Claire Milne, Appleby Global)

Businesses must be able to map the What? Why? Who? When? Where? for the personal data being processed.

Review and analyse:

- The personal data being processed
    - Ask what actually happens across the business – consult both senior management and front line staff about how personal data is obtained and used
- All documentation, fair processing information, website information, policies and procedures, staff awareness etc. that relate to compliance with the existing data protection legislation
- The current governance and security arrangements
- The retention of personal data (including archives)
- How the business manages the exercised rights of individuals, such as subject access requests, withdrawal of consent, opt outs from marketing

A toolkit to assist controllers
and processors is available on the website.

The GDPR represents a *"seismic shift in power relationships"* (Stewart Room, PWC Legal) and will *"usher in an era of greater accountability, with significantly increased transparency and controls for individuals to exercise management of their data".* (Phil Lee, Field Fisher LLP)

Improve practice

The GDPR may mean ***"end to end reform of business processes and practices"***
(Stewart Room PWC Legal)

Accountability, upholding rights and demonstrable compliance are key. All staff should be involved in tightening up and implementing procedures.

Management engagement

- Recognition of potential risk to business
- Recognition of impact on business processes
- Promotion and encouragement of compliance culture
- Encourage the input of staff
- Enable regular staff training/updating
- Consider appointment of an experienced data protection officer
- Monitor, test, review and improve practices and reporting mechanisms

Non-IT engagement

- Improve the information provided to clients/staff
    - Must be concise, transparent, intelligible and easily accessible, using clear and plain language
- Create records of processing activities
- Establish internal governance processes
- Ensure consent is clear and for explicit purposes
- Check the new rules around children's data are met, where relevant
- Identify any need for impact assessments
- Consider transfers to third countries

IT engagement

- Identify any automated decision-making or profiling
- Review customer facing processes for compatibility with the new rules on portability, access and restrictions on processing
- Build privacy by default into applications and processes
- Enable the identification and reporting of data breaches

"There are two years before the Regulation comes into force; two years to get ready, to look at practice and procedure, two years to tighten up."

(Tim Turner, Information rights trainer and blogger)