nccgroup

General Data Protection Regulation

Are you ready?

Prepared by: Lydia Lavender

1 Introduction

The EU General Data Protection Regulation (GDPR) will come into force across all member states (including the UK) on 25 May 2018.

Any doubts around what will happen post-Brexit were removed with the announcement last October (2016) by the Secretary of State for Culture, Media and Sport, Karen Bradley, that the UK will opt in.

Regardless of EU membership, the reach of the new regulation extends to any organisation providing services and/or goods to individuals within the EU, as well as those monitoring the behaviour of EU citizens.

The GDPR replaces the 1995 EU directive (Directive 95/46/EC) and begins a new chapter in European privacy.

This whitepaper will review the new controls against existing controls for the Data Protection Act 1998 [2] (DPA) and provide key next steps for businesses to undertake ahead of GDPR enforcement.

2 GDPR - what to expect

The following are some of the new controls the GDPR will introduce:

- **Scope:** The GDPR will apply to businesses within the EU and also to organisations outside of the EU if they process the data of EU residents.
- **Single set of rules and one-stop shop:** Each member state will establish a Supervisory Authority (SA), it is the Information Commissioner[3] for the UK, which will be responsible for their country but will work closely with the other SA's for any joint venture or operation.
- **Privacy by design:** Privacy must be built in to all new projects and initiatives including the requirement for privacy impact assessments (PIAs) to be conducted where specific risks occur to the rights of individuals.
- **Consent:** Valid and explicit consent must be given for all data collected and the purpose for its use must be fully explained. Opt-in options must be present for all data collection (supported by the current requirement in the Privacy in Electronic Communication Regulations 2003 [4] - PECR) and consent must be retractable at any time. Children under the age of 13 must have verifiable consent provided by a parent or guardian. This will have a major impact on marketing for all organisations and specific attention should be applied to this control.
- **Responsibility and accountability:** The current annual notice requirements remain and are expanded. They must also include the retention time for personal data and contact information for the data controller and data protection officer (see below).
- **Data Protection Officer:** Every organisation with more than 250 employees must nominate a dedicated data protection officer (DPO). The role will require the DPO to be proficient at managing IT processes, data security (including dealing with cyber attacks) and other critical business continuity issues around the holding and processing of personal and sensitive data. These requirements are in addition to understanding the legal compliance requirements of data protection laws and regulations.
- **Data breaches:** The GDPR will require the data protection officer to notify the SA "without undue delay" and within 72 hours of any breach of data security. Failure to notify of a breach could invoke a tier-two fine (see below) or higher from the SA. The notification should also include a risk assessment for informing data subjects of the breach if adverse impact is determined.
- **Fines:** A four-tier fine system will be put in place for breaches with the highest tier resulting in fines of up to €20 million (£15.8 million) or four per cent of global annual turnover (whichever is greater).
- **Right to erasure:** Also called the 'right to be forgotten', this control gives the data subject the right to require a business to permanently delete all information held about them on any one of a number of grounds.
- **Data portability:** A data subject shall be able to transfer their personal data from one electronic processing system to and into another, without being prevented from doing so by the data controller. This will include transfer between organisations as necessary (e.g. changing utility provider).

3 GDPR vs. DPA

Businesses in the UK are currently required to comply with the DPA 1998. The introduction of the GDPR will change some of the current requirements as well as introduce new ones. The table below shows how the GDPR requirements will affect their current counterpart controls:

GDPR	DPA	Impact
Scope: EU and companies with EU data subjects	The DPA currently applies to the UK only	Increase in scope and privacy requirements for non-UK data subject
Single set of rules and one-stop shop – SA in each country	The ICO is the governing body with complaints against the ICO going to the information tribunal	A single SA to monitor compliance with support from other SA's when required
Privacy by design – Privacy impact assessment (PIAs) for all projects and initiatives	PIAs should be conducted for new projects – not currently a requirement	PIAs are mandatory for all new projects and initiatives impacting privacy
Consent – opt-in for all data collections with clear and concise privacy notices	PECR requires opt-in but the DPA currently does not Privacy notices are required at all points of data collection	Requirement for opt-in for all data collection Privacy notices must be prominent and in plain English
Responsibility and accountability – notification requirements to include data retention and contact details	Annual notification to the ICO for data processing	Additional requirements for notification on an annual basis
Data Protection Officer – required for companies with more than 250 employees	No current requirement to have a dedicated DPO	A dedicated DPO must be in place for all organisations with more than 250 employees
Data breaches – mandatory notification within 72 hours	Notification is encouraged but not required	All data breaches must be reported to the relevant SA within 72 hours
Fines – up to €20m or 4% annual global turnover	Fines are currently up to £500,000 or 1% of annual turnover	Massive increase in potential fines for breaches or non-compliance
Right to erasure – removal of all records (including web presence) for a data subject	No current requirement to remove all data related to an individual	Systems must be reviewed and developed to allow deletion of specific records as needed
Data portability – ability to transfer data between electronic systems	No current requirement to provide ease of transfer between systems	New systems must be developed with portability as a requirement

4 Conclusion

The introduction of the GDPR brings an exciting new chapter in privacy. Individuals will be better informed and businesses will have to take better care of personal information.

While there may be some pain initially to prepare for the requirements, moving forward, privacy will become second nature and those who do it well could benefit from enhanced reputation with customers as well as lowering their risk of experiencing a security breach that could result in those new big fines.

Businesses have time to prepare for the GDPR but action should be taken sooner rather than later to understand your current position and create a roadmap to compliance.

GDPR is coming…Are you ready?

5 Next steps

The following are the top five steps that businesses should take to prepare for the GDPR:

1. Gain top level management buy-in as change must be driven from the top.
2. Conduct a current state assessment to understand your existing level of compliance.
3. Develop a security incident process and templates for notification of any breaches.
4. Create or update policies and processes for the protection of personal information.
5. Provide training for all employees so that they understand their responsibilities for protecting personal data and how to report a breach.

6 Further information

NCC Group is committed to helping clients prepare for GDPR. We offer a range of services from initial assessment through to transformation strategy.

For further information on our offerings and support on readiness for GDPR please contact: response@nccgroup.trust

We have authored a number of blog posts about GDPR and other relevant subjects and will continue to provide insight over the coming months. These can be accessed at: www.nccgroup.trust/GDPR

1. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
2. http://www.legislation.gov.uk/ukpga/1998/29/contents
3. https://ico.org.uk/