General Data Protection Regulation (GDPR)

Executive Headlines and Recommendations

25th May 2018 brings around the start of the enforcement of the new GDPR initiative which was initially adopted in April 2016, leading to the biggest shake up of privacy law in 20 years aimed to modernise data protection through clarity for businesses by implementing a single law for the EU.

Main Points:

- Mandatory for any company involved in the storage and processing of personal data of EU residents
- €20 million or 4% annual global turnover are the maximum fines for non-compliance
- Breach notification to regulator and affected individuals is mandatory
- Statutory liability to implement security measures to protect personal data
- Mandatory contractual provisions in data processing clauses and contracts
- Greater transparency and accountability around the processing of personal data

Who is going to be affected?

It is estimated that **98%** of member organisations will be impacted even though it is based on the same principles as the current data protection legislation it offers new rights to the data subjects as well as creating new roles for companies, like the needed Data Protection Officer (DPO) and the need to formally access data protection impacts.

Preparing for the GDPR

- A complete audit of information and processes that use personal data
- Privacy and data protection by design and default
- The implementation of unambiguous consent for any system that uses personal data
- Storage of detailed records of data processing, explicit consent and denials
- Implementation of personal data breach notification procedures
- Modify contracts with third-party data process to ensure GDPR compliance
- Aim to comply fully well before 25th May 2018

Data Protection Principles

The foundation of the worlds data protection regulations dictates that data held by organisations must comply with these principles:

- *Processed lawfully, fairly and in a transparent manner*
- *Collected only for a specific, explicit and legitimate purpose and not processed in a manner incompatible with the stated purpose*
- *Adequate, relevant and limited to what is necessary*
- *Accurate and kept up to date*
- *Held for no longer than is necessary*
- *Processed in a secure manner*

GDPR and other countries

- Data may not be transferred to jurisdictions that do not have equivalent data protection laws, unless legal safeguards are in place e.g. EU-US 'Privacy-Shield'
- Extends to EU residents' data no matter where it is being processed
- Covers all data processed in the EU no matter of subject's nationality or location
- GDPR can be enforced against an organisation even if it has no physical presence in the EU
- While Brexit means Britain will be leaving the EU one year after GDPR is implemented, however the GDPR will still be relevant due to the processing of personal data of EU residents

About the Legislation

- 200 pages of legal arguments and requirements
  - Two main sections
    - Introductory RECITALS
    - 11 chapters of the LEGISLATION

'So picking out the law from the many worked examples, recitals and case studies can be done by reference to what is actually quite short legislation.' Legal Counsel – Major Global Bank

Costs of GDPR compared to current legislation

Sample fines served for data protection breaches:

– TalkTalk Telecom Group PLC	£400k
– Cancer Research UK	£16k
– Moneysupermarket.com	£80k
– MyHome Installations Ltd	£50k
– Provident Personal Credit Ltd	£80k
– MacMillan Cancer Support	£14k
– Boomerang Video Ltd	£60k
– Guide Dogs for the Blind	£15k
– Greater Manchester Police	£150k

Last year the Information Commissioner's Office (ICO) collected £880,500 in fines from British organisations. However, if the GDPR regulation had been in place then the fines would have been on a totally different scale (up to £69m).

Consent to Process Personal Data

Consent is the primary method that organisations use to ensure a lawful basis for the processing of personal data, however the use of the 'opt-out' method is no longer acceptable. Organisations must now confirm consent through an **affirmative** action rather than simple inaction. So forgetting to tick a box is no longer valid consent. This also applies to data that is currently being processed, therefore organisations should ensure that evidence of consent is available. Additionally, a data subject under the age of 16 cannot give consent, requiring the parent or guardian.

Key GDPR Requirements

Applicability

- EU resident data is protected no matter the location of processing

Controls

Data Protection Officer

- An individual must be designated with responsibility for data protection

Data Protection Impact Assessments

- Assessments to situations of high potential risk to personal data

Data Transfers

- Suitable controls over personal data transfers to other organisations or countries must implemented

Capabilities

Legal Basis

- Evidence of consent from data subjects as this is the legal basis of processing

Breach Reporting

- Breaches must be reported immediately or within 72 hours of the breach being found

Consequences

- Supervisory authorities have new powers to investigate, fine or shut down data processing

Compliance

Organisations must comply by the 25th May 2018

Data Protection by Design

GDPR requires an organisation to adopt organisational and technical measures to deliver protection by design. The measures to be taken aren't specified, but the systems and processes must adopt privacy as a default, for example opting out of processing unless the data subjects want to opt in, or anonymising personal data.

Right to Erasure and Portability

The right to be forgotten is included, meaning that data subject can now ask to have their personal data erased without undue delay. It is required that organisations have the correct systems to identify, modify and erase personal data as well as the correct processes to prevent the restoration of erased data. Data subjects have the right to obtain their personal data in a format that is structured and machine readable this is intended to ensure that data is not withheld to make it difficult for a data subject to migrate to a new supplier for example a utility or telecommunications company.

The Ascot Barclay Group Approach

First and foremost, we recommend that rather than seeing this as a compliance exercise consider it more an overhaul of the way your organisation:

Like any overhaul there are three primary phases:

1. **LEGACY** – how do we do it now and what data have we got today? ***The current situation***.
2. **THE ASK** – as well as compliance with core GDPR obligations fold in enhancements that will yield better data performance given what, how and why we use data. ***The desired situation – goal***.
3. **GAP ANALYSIS** – the difference between 1 and 2 represent the gap and the program forms around bridging the gap to take us as speedily and efficiently as possible to our ***GOAL***.

And within these phases most, if not all, of the following activities will be required;

- Update Information Security Policy
- Develop awareness campaign
- Engage suppliers about GDPR
- Appoint Data Protection Officer, if required
- Assign database / file store business owners
- Information Audit
- Create a Record Retention Policy
- Adopt Data Breach procedures
- Data Protection Impact Assessments
- Processing personal data (demonstrable informed consent)
- Only use third-party Data Processors if they meet GDPR requirements
- Implement "Right to be Forgotten" & "Data Portability" procedures
- Implement "Data Protection by Design and by Default"

So how do you tie all this together and prove your organisation has at least tried to comply with the spirit of the GDPR? Fortunately **Article 24** of the GDPR says that organisations must implement "*appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.*" This article makes it clear that these measures must include implementing suitable information security policies.

The ISO/IEC 27001 Information Security Management System (ISMS) should be your starting point in seeking to ensure you can demonstrate "*appropriate technical and organisational measures…"* with respect to your GDPR obligations.

As ISO/IEC 27001 is the only independent, internationally recognised data security standard that also has a widely accepted certification scheme, it seems logical that ISO/IEC 27001 should be fundamental to your organisations GDPR strategy.

Regardless of *where* your organisation is on the route to compliance there is still time to make strides that not only ensure you fully comply but also realise hugely beneficial enhancements to the way you use data.

However time is short so please call ABG now on +44 (0)203 697 1364 or e-Mail tim.vincent@ascotbarclay.com for an initial conversation. We look forward to hearing from you.