Data Protection Act & GDPR Compliance

Introduction

The Data Protection Act (DPA) and the European version, the General Data Protection Regulation (GDPR) are designed to protect personally identifiable information and the rights of the individuals that are the subject of personal and sensitive information. Both regulations are legally enforceable (when the GDPR comes into force in 2018) and breaches of both, result in fines and prosecutions for the Data Controllers and Processors that gather, manage, control and process that data.

For GDPR breaches will incur fines of up to €20 million (or 4% of company turnover) and for breaches of the DPA fines of up to £500,000 can apply.

Most, if not all companies, hold personal information in the form of employee or customer personal records and therefore those companies must ensure that they are compliant with at least the Data Protection Act. For those organisation wishing to trade with the European Union, they should be getting ready to also comply with the GDPR.

Marathon offers an advice service to ensure that organisations have the policies, controls, processes and awareness, which will minimise any risk of a Data Protection regulation breach and prosecution.

Why Marathon?

Marathon's Information Security Group have vast experience of helping organisations assess the business risks associated with Cyber threats and security breaches through the use of best practice information security policies and procedures

Our consultants are Cyber Essentials Certified Assessors, ISO 27001 (information security standard) and ISO 22301 (business continuity standard) auditors.

Marathon's DPA & GDPR Advice Service

Marathon's approach to DPA and GDPR compliance is to firstly conduct an onsite workshop with relevant HR, Sales and Marketing and IT representatives within an organisation. The workshop is conducted by a senior Marathon Data Protection consultant and the session is used to understand what type of personal information is gathered, why it is gathered, how it is processed and how data subjects are kept informed of the information that is held and their rights relating to that data.

The Data Protection consultant will then produce a report highlighting the gaps between the company's current Data Protection practises when benchmarked with the DPA and if required, the GDPR. The consultant can present the report to board or senior management teams to discuss how gaps can be prevented and mitigate any Data Protection compliance risks that the company is exposed to.

Scope of Service

- Identify current activities that are regulated by the DPA and GDPR
- Ensure that the personal data being gathered is justifiable
- Ensure that personal data is being processed correctly, when relating to the justification
- Securing personal and sensitive information
- Handling requests for information and understanding data subject rights
- Controlling access to personal information
- Ensuring that adequate levels of transparency and privacy are in place
- Ensuring accuracy and currency of information
- Training and awareness relating to Data Protection compliance
- Breach management
- Main distinctions between the DPA and GDPR

Timescales

Typically the Data Protection workshop will take one day, with the report taking 2 days dependant on the size and complexity of the organisation in terms of their Data Protection exposure.

Other Services

Marathon's Information Security practice offer a number of valuable certification and enablement services including:

- Cyber Essentials Enablement
- ISO 27001 Auditing
- ISO 22301 Auditing
- Information Security Reviews

For more information speak with our Professional Services Team on 0208 329 1000
sales@marathon-ps.com

MARATHON PROFESSIONAL SERVICES