GDPR: compliance support for SMEs

Introduction

On 25th May 2018 the General Data Protection Regulation comes into force across Europe. The Regulation will be made law in the UK via The Data Protection Act 2018 (yet to be enacted) and takes penalties for non-compliance with data laws up to a maximum of 20 million euros or 4% of turnover, whichever is the greater. The vast majority of UK companies will need to prepare for compliance. Compliance with data privacy requirements will need to become a common part of business functions if companies wish to reduce their risk.

Main requirements

UK companies will need to manage their data more robustly than ever before. GDPR has strict rules on obtaining, processing, retaining and deleting personal data. The Regulation also allows for far greater subject access to data held.

Getting started with GDPR compliance

Companies would be advised to complete a full audit of the personal data and sensitive personal data that is processed by the business. Such personal data will be held on a number of different subject categories, for example, employees, customers, contractors. The audit will identify gaps in compliance and will lead to a range of actions in order to achieve compliance with GDPR. These activities can be prioritised to ensure any higher risk areas are addressed as a matter of priority.

Companies will need to review existing policies and, in all likelihood, create new supporting documentation. For example, a company's data protection policy will almost certainly require updating and new additional documents such as an information security policy and a data breach policy are likely to be required.

Employment contract clauses will need scrutiny as the traditional method on relying on consent for the processing of employee data is not the preferred or recommended approach under GDPR. Companies will need to think about how they inform their staff of their new rights (as data subjects) and responsibilities to the company (as employees) under GDPR.

Companies must also consider their relationships with third parties who might process personal data on their behalf. GDPR contains strict rules around such processing.

Help from Tridena

We are experts in data privacy and are certified information privacy professionals. We are able to provide advice on basic GDPR compliance up to complex international data sharing practices. We have developed a GDPR toolkit in partnership with a respected HR consultancy.

We offer the documents listed overleaf within a 'toolkit' to support you in becoming GDPR compliant. Purchase of the toolkit includes a one-hour telephone consultation to get you started with the audit and assessment exercise and to offer advice as you go. Any additional support required will be invoiced at the hourly rate normally charged for Tridena services.

GDPR toolkit – contents:

- Excel audit and assessment tool for data either i/ held specifically within the HR sphere or ii/ for data held across the company (whichever is required)
- Information and GDPR action checklist
- Template policy documents to be adapted to your company needs:
  - Data Protection Policy
  - Information Security Policy
  - Subject Rights and Subject Access Request Policy
  - Data Breach Policy
  - Data Retention Policy
- Template privacy notices for key data subjects to be adapted to your company needs:
  - Employees
  - Job applicants
  - Customers/clients
  - Employee referees
- Template clauses for third party processors to be adapted to your company needs
- Suggested employment contract clause replacing the standard 'consent to process' clause that many employment contracts currently contain

The documents have been prepared to assist client companies in their preparation for GDPR. Should you identify that further documents are required, please let us know and we will work to supply these to you. The documents are as thorough as possible but will need careful adaption by companies to ensure they are reflective of their business and operations.

The documents do not constitute legal advice and Tridena Ltd can accept no liability for negligence or error, or any loss caused by reliance on the information contained in the documents provided. Client companies are advised to familiarise themselves separately and fully with the GDPR to understand their organisational responsibilities.

Companies that engage in direct marketing should familiarise themselves with the provisions within GDPR specific to direct marketing activity and the e-privacy directive.

Explanatory notes have been added to the audit and assessment form, along with other documents where appropriate, but it should be noted that GDPR is complex so a reasonable knowledge of the provisions by the individual(s) overseeing the completion of this work within the business is recommended.

Cost: £500 + VAT

The above is supplied subject to Tridena standard terms of business. Should you wish to discuss this further, please contact Paul Davidson: paul.davidson@tridena,com.

Further information on GDPR can be found on the ICO website: https://ico.org.uk