5 top tips to prepare for GDPR

Description

Five tips for getting started to make sure you business is compliant

From 25 May 2018 the General Data Protection Regulation will be enforced. This enhances the rights of data subjects putting them back in control of their personal data and provides more obligations for data controllers to assist with this. To enforce this, the Regulator, in the UK the ICO, gets more powers to ensure that companies are complying.

The maximum fine will be â?¬20 million or 4 per cent global turnover and fines can be imposed for breaching the data protection principles but also for failing to have the correct administrative procedures in place â?? i.e. failing to report a breach which can attract an additional fine of up to â?¬10 million or 2 per cent global turnover.

In addition there is an obligation to report some data breaches involving personal data being lost, altered, destroyed, accessed either accidentally or unlawfully. If there is likely to a risk to the rights and freedoms of an individual then they must be reported to the ICO within72 hours of being discovered.

In addition if there is likely to be a high risk to the rights and freedoms of individuals then the breach must be reported to the data subject whose information has been affected.

1. **Start now.** Commence planning your General Data Protection Regulation change programme now as there are several steps required to ensure your organisation is compliant before May 2018.
2. **Find or hire someone that will make your GDPR problem interesting**. If you can make the problem compelling and the solution constructive, you will bring people on board with the change programme. The ideal person for the job will be someone who is working with customer data to develop insights for your organisation, as they understand how the business wants to use data.
3. **Identify which processes may cause harm**. Make a â??hit listâ?? of the processes that are most likely to cause harm to an individual, or the organisation. For example, a GP clinic managing health-related data could cause serious harm if patient data is mishandled, whilst losing the ability to send email marketing messages to your entire marketing database is also harmful. Once potentially damaging processes are identified, describe how the data flows through each process to visualise potential risks.
4. **Identify the external threats and internal errors posed to data management processes.** Have you used a third-party agency to create a data capture device, website or landing site? Make sure they are GDPR knowledgeable and can write programmes and privacy notices that comply with GDPR. Internally, your organisation needs to mitigate errors by ensuring staff are appropriately trained, and records of training are kept.

5. **Put an Information Governance Framework (IGF) in place**. An IGF includes a risk register that can help demonstrate your accountability by documenting how you review and act upon data management issues, especially by those with the appropriate levels of experience and responsibility.

Category

1. Compliance

Date Created
09/10/2017