Your simple six point guide to GDPR compliance

What is GDPR compliance?

A new data privacy law will come into effect in May 2018. It's called the EU General Data Protection Regulation (GDPR) and is a complete overhaul of the legal requirements which must be met by anyone involved in handling personal data of EU citizens.

The aim of the regulation is to give citizens greater control over what can be done with their personal data by businesses. This will be enforced by large fines – up to 20 million Euros or 4% of a company's global turnover – for non compliance.

The regulation must be observed by any organisation employing over 250 people. This implies that many SME's will be exempt. But that's not true. A business of any size must comply if it's involved in regular 'processing' of certain categories of personal data, which includes collecting and storing as well as using personal data.

The remit extends to paper based as well as electronic data with a forecast 40% of non compliance coming from paper based practises^. All businesses should support a paper security policy – including shredding facilities.

Full compliance will be important because the powers of the directive extend beyond the borders of Europe and apply to any business which handles EU citizen data, whether or not the business is based in the EU.

How does a business become compliant?

A lot of the GDPR obligations placed on businesses are common sense and should already be in practice in companies with solid data privacy and protection processes in place. However, here's a quick six point check list for compliance requirements:

1. Appoint a Data Protection Officer - keep records of all data processing activities performed by the company. This officer must be fully commensurate with the organisation's responsibilities regarding GDPR and have a thorough understanding of what data within your organisation counts as 'personal', where it's kept, who has access to it, how to spot breaches when they occur and who to report this to. The Data Protection Officer doesn't have to be an employee – you can outsource this function.
2. Assess your systems - Review all contracts, technology support, procedures and tools that relate to the processing, handling, storing and deleting of data to enable you to identify any weaknesses or gaps that require changes to be made.
3. Develop a strategy - Construct a new strategy that will ensure full compliance with the GDPR. This strategy may encompass new investment in technology, revise staff procedures and responsibility for data processing, create new roles within the organisation.
4. Implement a new organisation policy - The next step towards GDPR compliance is to put your plan into action throughout all levels of the organisation. Invest and introduce new technologies and systems required in the workplace and publish an informative data handling and processing guide.
5. Employee engagement – Launch your new data compliance policy to all staff; provide training, information and guides to employees so they are educated and aware of the changes taking place and their responsibility in ensuring that the company meets the requirements of the GDPR.

6. Review and improve - After launching your GDPR compliance plan, now is the time to review and improve before the regulations come in effect. Identifying any necessary improvements well in advance of the GDPR's deadline, once May 2018 arrives your organisation will have successfully and efficiently adapted to the changes and be completely compliant.

^ Source: Beyond good intentions: The need to move from intention to action to manage information risk in the mid-market, PwC report in conjunction with Iron Mountain, June 2014.

ENDS

692 words