Paper data breaches. How they happen and how to avoid them. The facts.

The EU's General Data Protection Regulation (GDPR) comes into effect in May 2018, requiring organisations to apply sound security practices to all electronic and paper-based personal data with respect to its collection, storage, access and disposal.

Part of the requirement is to put plans in place for what should happen in the event of a breach. Whilst electronic data security has been top of mind for many organisations for many years, the security of paper based personal data is often neglected or overlooked. **Statistics indicate that around 40% of data breaches will be paper based.**

In recent research, one quarter of employees admit to not shredding confidential information whilst two thirds of respondents said that managing the risks associated with paper records was a top concern for them+. Indeed, only 27% of companies surveyed reported policies for the safe security, storage and disposal of confidential personal information. ++

This puts organisations at risk of non-compliance and data subjects at risk of fraud and identity theft.

Paperwork still accounts for many common security breaches

According to the UK's data protection regulator, the Information Commissioner's Office (ICO) 40% of the 598 data security incidents recorded between July and September 2016 were attributable to paper breaches. These included loss or theft of paperwork (14%), paperwork posted or faxed to the wrong recipient (19%), data left in an insecure location (4%) and 3% due to insecure disposal of paper^.

From May 2018, non-compliance with the GDPR may result in fines of up to 20 million Euro or 4% of the company's global turnover, whichever is the greatest. That's a high price to pay for the lack of a suitable data compliance policy.

How to avoid paperwork breaches

Introducing clear rules about the use of paper documents containing information about an identifiable person and their personal data – defining what is 'personal' - and then the process for correct shredding of documents – based on the sensitivity of the data contained – is the first step towards compliance.

A clear and firm document shredding policy is required supported by robust GDPR compliance process.

+ 2014 PwC report in conjunction with records management company Iron Mountain, surveying European mid-market companies on their perception and management of information risk

++2014 PwC report in conjunction with records management company Iron Mountain, surveying European mid-market companies on their perception and management of information risk

^ 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

457 words