Practicing good business data protection

Bookmark this page

The first step to ensuring good business data protection is to identify all data in your business and where it's stored. Consider all places your data may be stored. It is increasingly likely that company data is also held outside your main IT system - on mobile devices or cloud services. Once you have identified all the data you hold, you can then evaluate its sensitivity and decide what steps to take to comply with data protection rules. A data protection audit is an ideal way to consolidate and organise this process.

Under the GDPR some organisations may have to appoint a data protection officer (DPO). A DPO can be an existing employee, a new hire, or the position can be contracted out. While not all organisations (especially smaller businesses) will require a DPO, it is good practice to have one person with specialist data protection knowledge within your business to oversee data protection compliance, conducting audits, data protection impact assessments for new projects, training relevant staff and raising awareness of data protection.

It's important you keep data accurate and up to date. Maintaining outdated records can be as bad as having no data at all, so implement procedures for regularly reviewing and updating records.

Duplicate records can be problematic too. You might end up mailing customers twice, or be unable to build up a picture of people's purchasing history. Many database systems allow you to identify duplicates automatically. If you store data about people - like customers or employees - you'll need to provide them with access whenever they request to see it, indicate how you're intending to use it and who the data might be shared with. Many businesses do this by establishing an area on their website where customers can log in, update their details and indicate their email marketing preferences.