General Data Protection Regulation - GDPR

Executive Summary

What is GDPR? GDPR replaces existing data protection laws and codifies and unifies data privacy laws across all European Union member countries. It came into effect on 25 May 2018.

Why does GDPR matter? Penalties for data breaches are potentially devastating. Serious breaches can incur fines of up to 4% of a company's global turnover. Note that breaches can occur not just because of malicious activity but can also include losses due to carelessness, inadequate procedures or system failures.

Who does GDPR affect? GDPR is applicable to any business collecting personal data from a citizen of the EU. The regulations require that breaches of personal data that may materially affect individuals must be reported to the UK Information Commissioner within 72 hours of the breach occurring.

What is Personal Data? GDPR uses the term *'personal data'* to describe information about individuals. It does not just refer to data that is stored electronically. GDPR includes paper documents that may be stored in a traditional filing system for example.

There are two key types of personal data identified under GDPR:

- **Personal Data.** Can be anything that allows a living person to be directly or indirectly identified. Examples are:
    - Name
    - Address
    - Computer (IP) address information
    - HR records
    - Customer contact details
    - Medical records
    - CVs
    - CCTV and telephone recordings
    - Appraisal records.

- **Sensitive Personal Data.** GDPR describes sensitive personal data as *'special categories'* of information. These include trade union membership, religious beliefs, political opinions, racial information and sexual orientation. The fines for breaches of sensitive personal data are potentially double for those of personal data.

What you can do to comply?

GDPR requires that personal data must be processed 'fairly, lawfully and transparently', in other words:

- personal data must not be used in a way that the individual to whom it relates would not expect;
- individuals must be informed how their personal data may be processed (for example, by way of a website privacy notice); and
- there must be a lawful basis for any processing, such as consent, or where the processing is necessary for the performance of a contract.

To help with compliance:

- Only keep the minimum amount of personal data you need.
- Decide on and implement a retention policy for personal data to ensure that documents are retained only for as long as necessary.
- Keep all personal data secure, use locked cabinets, encryption and password protection.
- Do not transfer personal data to portable storage devices or cloud-based storage, such as *Dropbox* or *OneDrive*.
- Do not print out personal data unless absolutely necessary.
- Lock your PC when away from your desk.
- Regularly change your password.
- Securely delete/destroy any out of date personal data. Shred do not bin.
- Do not use any personal data for any reason other than what it was provided for.
- Report any breach or loss of personal data.
- Do not pass personal data to any unauthorised third parties.
- Ensure laptops and all removable storage devices are encrypted and / or password protected.

What you should do if you suspect there is a data protection issue?

If you suspect that there may be a problem concerning data protection, you should escalate the matter promptly to the Data Protection Officer.