Risk Management: General Data Protection Regulation

Introduction

Europe is covered by the world's strongest data protection rules and the General Data Protection Regulation (GDPR) modernised the laws that protect the personal information of individuals. The GDPR is Europe's framework for data protection laws and it is on this that the Data Protection Act 2018 was based.

The Information Commissioner's Office (ICO) is responsible for enforcing GDPR. The ICO has the power to conduct criminal investigations and issue fines. It also provides organisations with large amounts of guidance about how to comply with GDPR.

How does it affect me?

Individuals, organisations, and companies that are either 'controllers' or 'processors' of personal data are covered by the GDPR and Data Protection Act 2018.

Both personal data and sensitive personal data are covered by GDPR.

- Personal data, a complex category of information, broadly means a piece of information that can be used to identify a living person either directly or indirectly. This can be a name, address, IP address. It includes automated personal data and can also encompass pseudonymised data if a person can be identified from it.

- Sensitive personal data is seen as being 'special categories' of information. These include trade union membership, religious beliefs, political opinions, racial information, and sexual orientation.

Accountability and compliance

Companies covered by the GDPR are accountable for their handling of people's personal information. This can include having:

- data protection policies;
- data protection impact assessments; and
- relevant documents on how data is processed.

Under GDPR, the "destruction, loss, alteration, unauthorised disclosure of, or access to" people's data must be reported to the ICO where it could have a detrimental impact on those who it is about. This can include, but isn't limited to:

- financial loss,
- confidentiality breaches, and
- damage to reputation.

The ICO must be told about a breach 72 hours after an organisation finds out about it and the people it impacts also need to be told. For companies that have more than 250 employees, there's a need to have:

- documentation of why people's information is being collected and processed;
- descriptions of the information that's held;
- how long it's being kept for; and
- descriptions of technical security measures in place.

Additionally, companies that have "regular and systematic monitoring" of individuals at a large scale or process a lot of sensitive personal data have to employ a data protection officer (DPO). They have to report to senior members of staff, monitor compliance with GDPR and be a point of contact for employees and customers.

There's also a requirement for businesses to obtain consent to process data in some situations. When an organisation is relying on consent to lawfully use a person's information they have to clearly explain that consent is being given and there has to be a "positive opt-in". The ICO website advises that there are multiple ways for organisations to process people's data that doesn't rely upon consent.

Access to your data

The GDPR also gives individuals a lot more power to access the information that's held about them.

A Subject Access Request (SAR), now available free, allows an individual the ability to ask a company or organisation to provide data about them. When someone makes a SAR, you must provide the information within one month. Everyone will have the right to get confirmation that an organisation has information about them, access to this information and any other supplementary information.

The regulation also gives individuals the power to get their personal data erased in some circumstances. This includes where it is no longer necessary for the purpose it was collected, if consent is withdrawn, there's no legitimate interest, and if it was unlawfully processed.

GDPR fines and the ICO

Under GDPR regulators have the ability to fine businesses that don't comply with it. This means you can be fined for:

- Not processing an individual's data in the correct way;
- Not having a data protection officer, when required; or
- A security breach.

In the UK, these monetary penalties will be decided by the ICO, which previously could fine up to £500,000. Smaller offences could result in fines of up to €10 million or two per cent of a firm's global turnover (whichever is greater). More serious consequences can have fines of up to €20 million or four per cent of a firm's global turnover (whichever is greater).

However, the intention of the ICO remains to work with organisations to improve their practices. Companies that have shown awareness of the GDPR and tried to implement it will be supported; those that haven’t are likely to find a firmer approach being adopted.

What should we do to comply?

Data protection requires continual attention to demonstrate you are striving to comply.

Keeping on top of data can be a tricky thing – especially when businesses are evolving the services that are offered to customers. The ICO's guide to GDPR sets out all the different rights and principles of GDPR and the advice for small organisations can assist in getting things rights at the outset.

Otherwise contacting the ICO or attending one of their webinars is the best way to ensure you are fully compliant.