Data Protection Act 1998

The Data Protection Act 1998 (DPA) is designed to protect a person's information, or data. It attempts to balance the right of an individual's privacy against the need for organisations to use personal information in the course of their business.

Data protection can pose a real risk to your business both financially and in terms of your reputation. Any accidental or deliberate loss or destruction of data could result in a substantial financial penalty. It can also be used as a tool; as individuals become increasingly aware of their rights under the DPA they can request copies of their personal information which can delay proceedings and prove a costly and time consuming exercise for businesses.

The Information Commissioner's Office (ICO)

The ICO was set up to uphold information rights and regulates compliance with data protection law. It has extensive powers should a breach of data protection occur which can result in a fine of up to £500,000. Imminent changes to data protection law are due to increase this amount to a percentage of worldwide turnover resulting in potentially much higher penalties depending on the nature of the breach. If managed correctly, the response to a breach together with having appropriate policies and procedures in place can substantially reduce any monetary penalty or avoid it altogether.

Data Protection Principles

The DPA contains eight principles under which organisations must process personal data. These include the need to process the information fairly and lawfully, ensure the information is adequate for the purpose, is accurate and kept up to date. Further requirements include the transfer of data abroad, the security of all data and individuals' rights under the DPA.

What is Personal Data?

Information relating to a living individual who can be identified from that information or identified from that information when combined with other information you already hold or may hold in the future. Sensitive personal data includes information such as medical records and is subject to more stringent processing rules.

Who is a Data Subject?

Every living individual about whom you hold information whether they are employees, clients, suppliers, stakeholders or other individuals.

Are you a Data Controller or Data Processor?

Whether you are a data controller or a data processor can significantly impact on the level of responsibility you have in relation to the personal information you hold. A data controller determines how data is collected and the purposes for which it is used. A data processor processes the personal information on behalf of the data controller. In some cases it may be that you are acting as data controller and data processor.

What should you do to ensure compliance and minimise risk?

- Register with the ICO – this can be completed online and usually costs £35
- Appoint a senior member of staff to have responsibility for data protection

- Ensure you have an up to date data protection policy and appropriate procedures
- All staff should receive initial and refresher data protection training
- Audit your business to assess and identify any gaps in data protection practice
- Consider encryption particularly if you are dealing with a high volume of data or the data concerned is of a sensitive nature. Although not specifically required under the DPA, principle 7 does require certain standards to be met and the ICO has issued financial penalties where there has been a loss of data and no attempt at encryption has been made
- Create a breach management plan
- Consider your company insurance. Some Director and Officer policies will provide cover in the event of a penalty being issued, other specialist insurance is available purely in relation to data protection

Future developments?

The General Data Protection Regulation (GDPR) is a proposed reform of the existing law, the framework for which was approved at the end of 2015 and which is intended to replace the DPA within the next two years. Proposed changes will include an increase in financial penalties following breach and strengthening of individuals' rights.

Existing rights for individuals

One of the most used rights by employees is the right to access a copy of their data by way of a subject access request (SAR). Complying with these requests has become ever more onerous given the increase in information collected and digitally stored by organisations. It is also worth noting that this right also includes a right to a copy of all relevant telephone recordings and CCTV footage.

Identifying a SAR

Responsibility in recognising an SAR lies with the organisation. A request does not have to refer to the DPA or make any reference to the words 'subject access request'.

Consider the following: *Please send me copies of all written evidence including all witness statement at your earliest convenience and without unreasonable delay*

Responding to a Subject Access Request

- A response in 'intelligible form' to be made within 40 days (subject to receipt of ID and fee)
- Electronic files and some paper files (if in structured form)
- Consent to disclose third party data and/or is it 'reasonable in all the circumstances'
- Consider redaction of information
- Consider if any exemptions apply

If an individual is not satisfied with a response it can refer to the ICO for review.

Contact us:
Banbury office: 01295 270999
Bicester office: 01869 252161
London office: 0203 7553247
Rugby office: 01788 579579