SME Business Guidance Series

The Eight Principles of the Data Protection Act

Provided by:

Crendon Insurance Brokers

www.crendoninsurance.co.uk

enquiries@crendoninsurance.co.uk

11 Greenfield Crescent, Edgbaston, Birmingham B15 3AU
Tel: 0121 45 45 100

Follow us on LinkedIn:

Follow us on Twitter:

Since the Data Protection Act 1998 (DPA) came into effect in March 2000, businesses and organisations have had to follow eight data protection principles when processing sensitive and personal data. Noncompliance with these principles can carry fines of up to £500,000 from the Information Commissioner's Office (ICO) and possible compensation claims by individuals. Following is guidance from the ICO on how to comply with the eight principles of the DPA.

Principle 1: The persona data must be fairly and lawfully processed.

- Have legitimate grounds for collecting and using personal data.
- Do not use the data in ways that have unjustified adverse effects on the individuals whose data you are processing.
- Be transparent about how you intend to use the data and give individuals appropriate privacy notices when collecting personal data.
    - A 'privacy notice' (oral or written statement) should state the organisation's identity, purpose for using the information, and any extra information needed to enable fair processing of the information. For more information on privacy notices, please see the ICO Privacy Notices Code of Practice at www.ico.gov.uk.
- Allow individuals to decide whether to supply the personal data, and make sure they have a clear understanding about what the data will be used for.
- Handle an individual's personal data only in ways he or she would reasonably expect.
- Do not do anything unlawful with the data.

This principle also requires organisations to satisfy a 'condition for processing', such as gaining consent when processing personal data and gaining explicit consent when processing sensitive personal data. The full list of conditions is set out in Schedules 2 and 3 of the DPA.

Principle 2: The personal data shall be processed only for specified and lawful purposes.

This principle closely aligns with the first principle.

- Be clear from the outset about why personal data is being collected and about your intentions with the data.
- Comply with the DPA's fair processing requirements, including the duty to give privacy notices to individuals.
- Comply with ICO notification procedures.
- Ensure that if there is an additional or different use or disclosure of personal data that differs from the original specified purpose, the new use or disclosure is fair.

Principle 3: The personal data shall be adequate, relevant and not excessive.

- Ensure that the personal data held is sufficient for the particular purpose.

- Store no more information than necessary for the particular purpose.
    - Create a data strategy with clearly defined purposes for each set of data.
- Practise 'data minimisation'—identify the minimum amount of personal data needed to fulfil the purpose.
- Take into account that 'adequate, relevant and not excessive' may differ from individual to individual.

Principle 4: The personal data shall be accurate and kept up to date.

- Take reasonable steps to ensure the accuracy of any personal data obtained.
- Ensure that the source of any personal data is clear.
- Carefully consider any challenges to the accuracy of information.
- Consider whether it is necessary to update the information.
    - A system for updating should be in place if the data is required to be up to date.

Principle 5: The personal data shall not be kept for longer than is necessary.

- Review the length of time personal data is kept.
    - Consider the purpose for holding the information when deciding how long to retain it.
- Regularly review personal data being held to determine if it is still needed. Create a data retention policy if holding large amounts of data.
- Update, archive or securely delete out-of-date information.
    - Securely delete information that is no longer needed.
    - Make proper provisions for deleting physical records and electronic records that could be encrypted.

Principle 6: The personal data shall be processed in accordance with the rights of individuals (data subjects).

The DPA grants individuals rights when their personal data is processed. The most common individual right used is the subject access request, or request to see one's held personal data. A data controller has 40 calendar days to comply with the request and may charge up to £10. Businesses should have a process in place when dealing with written requests for information and processing. Individual rights the sixth principle refers to are:

- The right to access to a copy of information containing personal data
- The right to object to processing that is likely to cause or is causing damage or distress

- The right to prevent processing for direct marketing
- The right to object to decisions being made by automated means
- The right to have inaccurate personal data rectified, blocked, erased or destroyed in certain circumstances
- The right to claim compensation for damages caused by a breach of the DPA

Principle 7: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

This principle relates to information security and protecting personal data from becoming lost, stolen or hacked. In practice this means that a business must have the appropriate security to prevent personal data from being accidently or deliberately compromised.

Businesses should:

- Design and organise the security to fit the nature of the personal data and the harm that may result from a breach.
- Be clear about who is responsible for ensuring information security and carry out an information risk assessment.
- Ensure adequate physical and technical security, backed up by robust policies, procedures and a well-trained staff.
- Be ready to respond to any breach of security swiftly and effectively.
    - If personal data is lost, altered or destroyed, have a recovery plan in place to prevent further damage or distress to the individuals concerned.

Principle 8: Personal data shall not be transferred outside the European Economic Area (EEA) without adequate protection.

A business cannot transfer personal data outside of the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal data.