Checklist
Data protection

This checklist highlights the key legal obligations your business should consider when dealing with personal data about:

- Customers
- Suppliers
- Employees
- Any other individual who you may encounter in the course of business

1 Penalties for failing to deal with personal data appropriately

- There could be serious financial, commercial and reputational implications for your business (including possible criminal penalties and fines) if personal data is not handled properly.

2 Protecting and securing personal data

- Personal data is any information about an individual held on computer or in organised filing systems that could identify the individual, either on its own or together with other information your business or a third party holds. It needs to be protected and kept secure. This information includes:
  - Name
  - E-mail address
  - Telephone numbers
  - Date of birth
  - Notes written about someone (such as an annual performance review).

- You must take particular care with sensitive personal data (for example, medical records) as more restrictive requirements apply to this type of data.

- The individual could be a potential or actual employee, customer or supplier, or possibly someone captured on your business's CCTV footage.

3 Collecting personal data

- Your business can only collect personal data if it has a legitimate reason for doing so (for example, because a new employee is coming to work for you).

- When your business collects data about an individual, you will need to tell that individual what your business intends to do with their data (for example, if you are collecting a customer's e-mail address to confirm an order). If the purposes for which you want to use someone's data change later, you must approach them again.

- Your business should only collect information it requires at the particular time (for example, a job applicant should not be asked for their bank details). This type of data should only be collected once the applicant has started to work for your business.

- If your business wants to use someone's data for marketing purposes the individual must be informed. It is good practice to do this at the time the data is collected. In some cases (such as text or e-mail marketing) your business generally needs the individual's explicit consent.

4 Using data collected on individuals

- Your business is generally allowed to use someone's personal data if they have given their consent. The data can also be used in other circumstances, for example, if your business:
  - Needs to use the data to fulfil a contract with a customer (such as using their address to deliver goods to them)
  - Has a legitimate interest in using it, although this must be balanced with the individual's rights. For example, if a part of your business has been sold to a third party and you need to transfer customer data to it.

- Data should only be used for the reason that it was collected (for example, if calls between staff and customers are recorded for training purposes only, they should not be used to discipline a member of staff).

- If you want a third party to manage data (such as carrying out payroll services) you should take legal advice. Your business will still be responsible for protecting the data and will need to enter into a written contract with the third party.

- Your business should also take legal advice if it is considering transferring any data outside the countries

Checklist
Data protection

in the European Economic Area. It is very easy to transfer data outside of your own country (for example, by sending an e-mail to an office outside of the UK).

- If the data is being used in marketing material, check that the recipient is aware that their data may be used for this reason and confirm they do not object. You will generally need the individual's explicit consent (opt-in) for e-mail, fax and text marketing. If the individual is an existing customer, you may be able to market similar products to them by these means without prior explicit consent. You should take legal advice if you want to do this.

- If your business is considering using sensitive personal data (for example, information about ethnic origin, trade union membership or criminal records), you should take legal advice.

5 Storing personal data

- All data must be accurate and up to date. Databases should be regularly cleaned and out-of-date information must be deleted.

- Data should only be held for as long as it is required and for the reason it was collected. For example, if personal data was collected to deliver a product a year ago and not used since, it should not be held on the basis that it may be needed for another reason at some time in the future.

6 Keeping data secure and confidential

- Personal data must be kept secure at all times. For example:
  - Computers and files should be password protected
  - Personal data on laptops and other portable devices should be kept to a minimum
  - Manual filing cabinets containing personal data should be locked and only accessible to authorised personnel
  - Confidential documents should not be left unattended on desks
  - Personal data should be removed promptly from fax machines, printers and photocopiers.

- When your business sends personal data, it must be done in a secure way (for example, confidential information should not be sent in the internal mail).

- Personal data must be disposed of securely (for example, by shredding, placing in confidential waste bags, destroying or securely deleting electronic files). Confidential papers should not be put in the recycling bin.

- When working away from the office or in public areas:
  - Ensure personal data stored on portable devices such as laptops, Blackberries, CD-ROMs or memory sticks is encrypted and kept secure at all times
  - Avoid leaving papers or electronic devices lying around
  - Make sure members of the public cannot see confidential documents or computer screens
  - Avoid talking about confidential matters when the public can hear.

- Security breaches (such as accidentally losing personal data) should be reported to the appropriate person immediately.

- Electronic documents, including calendar entries and meeting requests, should be password protected or designated private where appropriate.

7 Enquiries about personal data

- Make sure your business has a system in place to deal with individuals who request details of the personal information your business holds on them. You are permitted to charge an administration fee of up to £10 for responding to this type of request.

- Individual employees should not deal with this type of enquiry, unless they have been given specific authorisation to do so. The request should normally be passed to the person within your business who has responsibility for data protection issues.

- Personal data should not be given out to the friends or relatives of an individual without that individual's specific consent.