data protection

This checklist highlights the key legal obligations your business should consider when dealing with personal data. Failure to handle data properly could lead to serious financial, commercial and reputational implications for your business including possible criminal penalties and fines.

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. It needs to be protected and kept secure.

This information includes:

- name;
- e-mail address;
- telephone numbers;
- date of birth; and
- 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' CCTV footage.

Collecting personal data

Your business can only collect personal data if it has a legitimate reason for doing so.

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 or to send marketing material).

If the purposes for which you want to use someone's data change later, you will have to 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).

More information

If you have any queries about the content of this checklist, please contact Amanda Doyle on **amanda@doylelaw.co.uk**.

Using data collected on individuals

Your business is generally only allowed to use someone's data if they have given consent, although it can also be used in some 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); or
- 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) your business will still be responsible for protecting the data and will need to enter into an appropriate written contract with the third party. If necessary take legal advice, particularly if you are considering transferring any data outside the countries in the European Economic Area.

Marketing

If the data is being used to send marketing material, check that the recipient is aware that their data may be used for this reason and confirm they do not object.

For e-mail, fax and text marketing you will generally need an individual's explicit opt-in consent. However, there is an exception to this, known as the 'soft opt-in'. Provided you meet the following criteria when you will be able to send e-mail, fax and text marketing without opt-in consent:

- you must have obtained the individual's details in the course of a sale or the negotiations for a sale of a product or service to that person (you do not need to have actually sold something they need only have expressed and interest).
- the messages are only marketing your similar products or services; and
- the individual is given a simple opportunity to refuse the marketing when their details are collected and, if they do not opt out, you give them a simple way to do so in every future message, e.g. "unsubscribe" button or respond with "stop".

Direct mail by post and cold-calling are subject to additional rules and you must check whether an individual or company has signed up to the mailing/telephone preference service through which they indicate that they do not wish to receive such marketing.

Details collected from your website

If you use your website to collect personal data, the website should include a privacy statement with a fair processing notice i.e. a notice explaining what you will use their data for (for example, marketing and whether you will pass the personal data to third parties for marketing purposes).

If your website uses cookies you must also obtain the users consent to the cookies.

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.

More information

If you have any queries about the content of this checklist, please contact Amanda Doyle on **amanda@doylelaw.co.uk**.

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; and
- 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.

Personal data must be disposed of securely (for example, by shredding, placing in confidential waste bags, destroying or securely deleting electronic files).

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; and
- 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.

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.

More information

If you have any queries about the content of this checklist, please contact Amanda Doyle on **amanda@doylelaw.co.uk**.