Personal Data Guardianship Code

Duties of the Responsible person 7
Responsibilities of the Data Handler 10
What you can do about your personal data 12
Every organisation that handles personal data should have in place specific rules and procedures which protect the rights of the people whose data it holds. This Personal Data Guardianship Code is intended to help organisations and the people in them who handle personal data understand their individual responsibilities. It aims to promote best practice and provide ‘common sense’ guidance, in the same way that the Highway Code provides guidance to motorists to enable them to drive safely for the benefit of both themselves and other road users. This Code of good practice aims to assist organisations to comply with the law and will also help the general public to understand how to protect their personal data.

What is personal data and why is this Code necessary?

Our personal data is data about ourselves that identifies us directly or indirectly and that we may wish to keep private, such as our mobile phone number or financial information. Particularly sensitive personal data such as our medical history or religious beliefs is given additional protection under the Data Protection Act 1998 (DPA). Personal data is held by many organisations (for example central and local government, hospitals, health centres, banks, retail stores, service providers and social networks). This means that all living individuals are data subjects in legal terms, as defined in the DPA. When we die, our information ceases to be personal data in the eyes of the law.

We should all recognise the value of our personal data and also treat other people’s personal data as we would wish them to treat our own. All organisations holding personal data (data controllers in DPA terms) have legal obligations under the DPA to ensure that this data is managed well.

This Code recommends that each organisation should appoint at least one senior-level responsible person who is accountable for the purpose and manner in which personal data is collected, processed, stored and disposed of. Workers across an organisation, because of the nature of their roles, may also act as data handlers to manage personal data.

The DPA contains eight data protection principles. These state that personal data must be:

1. processed fairly and lawfully and in compliance with the detailed conditions in the DPA;
2. obtained and used only for specified and lawful purposes;
3. adequate, relevant and not excessive (for those purposes);
4. accurate, and where necessary, kept up to date;
5. kept for no longer than necessary;
6. processed in accordance with the individual’s rights;
7. kept secure; and
8. only transferred to countries outside the European Economic Area (EEA) that offer an adequate level of protection. The EEA comprises the countries of the European Union plus Iceland, Liechtenstein and Norway.

The impact of these principles on the processing of personal data is illustrated by the examples given in this Code.

Example 1: To ensure your newspaper is delivered, your newsagent can create a database containing your personal details and subscription records. The DPA imposes the same basic obligations on the newsagent as on a large private or public sector organisation to manage your personal data well.

Example 2: Information about a party at home posted on a social networking site may result in hundreds of ‘uninvited’ guests arriving at your home, unless you ensure that the privacy settings restrict the information to those you would choose to invite.

Example 3: You may be in the habit of sending personal emails from work, but your employer has a legal right to look at your personal emails sent or received using their equipment if there is a business justification and this has been explained to you. Your employer may have asked you to sign an acceptable use policy in relation to email. In exceptional circumstances this may give the employer the right to access and read personal data that you have sent in an email at work to a friend or vice versa.

Example 4: Online retailers collect mobile phone numbers and email addresses of their customers so that they can contact them in the event that there are problems with supply or delivery of the ordered goods. However, the retailer should not use these channels to send marketing messages to customers without having received consent. Neither can they retain this information for their own use after the transaction is completed except as required by law as, for example, for financial audit purposes.
Structure of the code

This Code identifies the principles and responsibilities on which ‘best practice’ is based. The data life span is shown below and is described in detail in this booklet. The three reference sheets provide an alignment of the Code with the roles and responsibilities of the responsible person and the data handler and give an overview of how an individual data subject can protect their personal information. Refer to ‘What is personal data and why is this Code necessary?’

Key references

The key acts and regulations that this Code is based on are: the Data Protection Act 1998, the Human Rights Act 1998, the Freedom of Information Act 2000 and the Privacy and Electronic Communications Regulations 2003. Other UK and EU legal rules and work led by BCS to develop a simple and consistent framework for handling personal data have also been drawn on.

The data life span

Personal data is normally collected in order to provide some service to the data subject. Personal data goes through a three-stage handling life span: input, use and output, as shown in the diagram below, together with its components and processes.
The principles of good data governance

‘In each situation the collection and use of personal data has to be considered from the perspective of the eight principles.’

Accountability

Processing personal data means collecting, recording, holding or sharing the data, or using it in any other way. This is a very wide definition.

All those holding personal data should follow data governance principles that include clear management responsibility, authority and the procedures for collecting, retaining, identity matching, sharing, disseminating, disposal, risk assessment, security and audit of the data. These principles should be available to the public. If this is done correctly, it will foster public trust and safeguard the personal data within an organisation’s care.

Example 5: An organisation that sends an unencrypted CD containing sensitive personal data by post is clearly not following sound governance procedures for protecting personal data held in their charge. People who should be considered at fault are: (1) the board, who are ultimately responsible for ensuring adequate policy is set, (2) the responsible person who is accountable for ensuring that policy is applied and (3) the data handler who sent out the CD if this is in breach of company policies.

Visibility

Data subjects have the right to know who is holding their data and so it is essential that, when personal data is collected, it is clear which legal entity is requesting the information, how they will use it and to whom they may disclose it.

Subject to some legal exceptions, data subjects also have the right to be informed of and to access all personal data about themselves that an organisation holds. An organisation is entitled to make a nominal charge for this. Data subjects have the right both to correct this data if it is wrong and to know who has had access to it.

Example 6: A retail company trades under different brand names. Whenever personal data is collected you must be told the legal name of the retail company behind the brand beforehand.

Example 7: You have the right to see your personal data held by credit rating agencies and the right to correct the data if you can demonstrate that it is wrong. Even if the agency disagrees with your correction, it must include a ‘notice of correction’ on your file.

Consent

In each situation the collection and use of personal data has to be fair and lawful and in accordance with the eight data protection principles. There must be a proper basis for processing personal data, meeting one of the conditions for processing set out in schedule 2 and (where sensitive personal data is concerned) schedule 3 of the DPA (see ‘What is personal data and why is this Code necessary?’). The most common condition is where the individual has agreed to the use of their data.

Individuals should be given as much control as possible over how their personal data is used and disclosed. This means, before individuals provide their personal data, giving them sufficient clear information about how their data is going to be used, the consequences of consenting to such use and obtaining the individual’s clear consent to this where appropriate.

Example 8: Your employer is obliged by law to pass on data relating to your earnings to HM Revenue and Customs and getting your consent to this is clearly meaningless. However a request for your earnings details from a building society to verify a mortgage application would require your clear consent before these details could be passed on.

Otherwise, personal data should only be used for the purposes to which the data subject has consented. If the collecting organisation wishes to use the personal data for another purpose or pass it on to a third party, the data subject’s consent should be explicitly obtained beforehand, unless the organisation can rely on one of the conditions in the schedules mentioned above.

Example 9: The delivery address provided to a retailer during the purchase of a washing machine should not subsequently be used for sending marketing material about a holiday or be passed on to a third party without first obtaining the data subject’s consent.

Example 10: Failure to provide a minimum of personal data (such as a home address) may result in a supplier being unable or unwilling to enter into a delivery contract with the data subject.

Where uses or disclosures of sensitive personal data, such as medical information, are contemplated then such uses must be explained before explicit agreement is sought through a signature or some other active indication. Normally, a patient’s consent for disclosure of their information to the doctors and nurses who are treating them may be presumed.
Example 11: If a patient who has been told how their medical information will be used withholds consent to access their medical records, they should be made aware that a hospital may not be able to provide the level of medical care that access to a full medical history would allow. However, a patient is normally entitled to withhold particularly sensitive information, unless this would seriously compromise the treatment of someone else.

Example 12: A physiotherapist collects information about your health before treatment. You should be told why the information is needed and then asked to sign the collection form or some other consent form. There are circumstances in which consent may not be necessary. These are explained in the DPA, however, if an organisation chooses not to use consent then you should normally be made aware of what other DPA condition of collection is being satisfied so that you can challenge this if you feel it is not justified.

Example 13: A council asks you to provide your ethnicity when you apply for a library card. You should be told why they are doing this and whether they will link your ethnicity to your use of the library, or whether they are collecting this separately to monitor take-up of the library service by ethnic groups, without linking this to you as an individual.

Access
Organisations should specify what types of personal data are processed and to whom they may be disclosed.

There should be an audit trail within an organisation showing who has actually accessed personal data. Access to sensitive personal data (such as health, sexuality, religion or membership of organisations like trade unions or political parties) should be permitted only if the individual’s consent has been obtained or another lawful condition applies.

Example 14: Not all staff working in a medical clinic should have access to a data subject’s identifiable medical records. These should only be accessed by staff directly engaged in the data subject’s care and treatment.

Example 15: The girl guiding database holds personal data on all girls and adults involved in guiding. It is the policy of the Guide Association that all personal information will only be used for guiding purposes and will never be passed on to a third party.

Stewardship
Those collecting personal data have a duty of care to protect it throughout the data lifespan. They need to ensure that anyone using it understands the risks associated with its use, the purposes for which consent has been obtained (where relevant) and its accuracy, for example whether the personal data has been verified or is interpretation and hearsay; when it was collected; if it has a finite useful life; and if it has been cleansed.

Personal data should not be passed on to a third party, unless the organisation that originally collected the personal data ensures that any caveats associated with their use of the data are passed on and permission has been obtained from the data subject if necessary (see Example 9).

Example 16: Many organisations outsource some support services, for example payroll, to a subcontractor (‘data processor’ in DPA terms). Where an organisation commissions a subcontractor to process personal data for it, the responsible person of the subcontractor should ensure that the uses of the data are restricted to those established by the responsible person of the commissioning organisation, which, as the data controller, is ultimately accountable under the DPA.

Stewardship also extends to ensuring that appropriate care is taken of personal data in cloud computing.

Example 17: A community nurse proposes uploading clinical details of the patients she visits onto a public cloud service, which would be accessible to her colleagues and to other social services and emergency services personnel. The aim would be to provide critical care information that would greatly improve service to patients. She is advised that this would pose an unacceptable risk as the security of very sensitive personal data could not be guaranteed. An alternative scheme using a private network or cloud with appropriate security measures (such as strong encryption) would be more suitable.

Example 18: An organisation proposes to use a cloud computing service based in California, which doesn’t offer the data protection rights required by the European Union Directives and Regulations. The organisation should endeavour to agree a contract with the service provider that provides adequate rights or consider using an alternative service that does offer such rights.
Responsibilities

All organisations should have an agreed and documented policy on data assurance (security) and data privacy that is compliant with the DPA. This policy should set out the governance arrangements for data assurance and privacy. Good governance makes clear who is accountable (the board) and to whom the board has delegated aspects of accountability (the responsible person) for the compliant management of all personal data. Ultimate responsibility rests with the board in a private sector organisation, the accounting officer in a public sector organisation and the trustees in a charitable organisation.

The responsible person should be appointed by the board and can delegate to other workers in the organisation the authority for all or part of the processes in the data lifespan, for example data input, data correction or data disposal. It should be clear, at all points in the data lifespan, who has been authorised to handle personal data and the extent of their authorisation.

Organisations holding personal data have a responsibility to ensure its accuracy and relevance and to put effective processes in place to review, maintain and dispose of it. They also have a responsibility to collect and hold only the minimum of personal data needed for the service(s) offered.

Example 19: A delivery company needs to know the name, address and telephone number of a customer, but does not need to know the customer’s religious beliefs.

Example 20: While occupational health staff may need to know the employee’s medical history, they do not need to know the employee’s salary. The HR department should not share this with them.

An individual handling personal data (the data handler) needs to know who, in their organisation, is ultimately accountable for that personal data (the responsible person). The data handler must also be clear about what they, as an individual, have been authorised to do with that data. The authorisation should be in writing and not an ‘informal’ arrangement or request. The data handler should never exceed their authorisation and should always query anyone who asks them to exceed it. If the data handler becomes aware of a compliance failure, they should alert the responsible person.

Example 21: One method of controlling access to information is by providing staff with a log-on to only the required functions of a system. Provision of a log-on explicitly limits the authority of the staff member to access and process personal data. To ensure that accountability is maintained, the log-on should be associated with a named individual. A shared/guest log-on should not be used to allow access to personal data.

Disclaimer

This Code is not intended to be relied upon as giving specific legal or other advice, and where the reader is unsure about any aspect of the DPA or other legislation they should seek legal advice or visit the website of the Information Commissioner. Whilst every care has been taken by BCS in the preparation and publication of this Code, no warranty is given by BCS as to the accuracy or completeness of the information contained within it and BCS shall not be responsible or liable by reason of any breach of contract, negligence or otherwise for any loss or damage whatsoever arising by virtue of such information or any instructions or advice contained within this Code.
Duties of the responsible person

All organisations holding personal data must designate at least one senior-level responsible person, who is accountable for personal data. Where an organisation has multiple business departments there may be a separate responsible person for each business department. The organisation should also have a data assurance and privacy policy. This policy should set out the governance arrangements for data security and privacy. Whilst everyone who processes personal data is responsible for complying with best practice, ultimate accountability rests with the board in a private sector organisation, the accounting officer in a public sector organisation and the trustees in a charitable organisation.

Good governance makes clear who is accountable (the board) and to whom the board has delegated aspects of accountability (the responsible person) for the compliant management of all personal data.

The responsible person can delegate to other people and outsourcers the authority to manage all or part of the processes in the data lifespan, for example data input, data updates or data disposal. It should be clear, at all points in the data lifespan, who has been authorised to handle personal data and the extent of their authorisation. Even though an organisation may have outsourced the processing of personal data to a third party, the organisation remains responsible for the compliant processing by that third party and should ensure compliance by means of contractual obligations.

Organisations that use personal data have a responsibility to ensure the accuracy and relevance of that data and to have effective processes in place for its review, maintenance and disposal. Organisations also have a responsibility to collect and hold only the minimum of personal data needed for the service(s) offered.
Duties of the responsible person

**Input - collection, verification and cleansing**

**Accountability**
The responsible person is accountable to the board for the collection, maintenance and handling of personal data within their area of the organisation. This means that the responsible person must ensure that:

- the purpose(s) for which personal data is being captured and used, and with whom and why the data will be shared are clearly stated;
- appropriate governance procedures, including undertaking a risk assessment or privacy impact assessment, are in place to safeguard the data and its use throughout the data lifespan;
- the personal data collected by their organisation is relevant for the stated purpose(s).

The responsible person in an outsourced or third-party supplier is accountable for ensuring that their organisation abides by data protection principles and complies with the contractual obligations imposed by the original organisation.

**Example 22:** A retailer uses a marketing organisation to collect customer information. The retailer must ensure that the marketing organisation is contractually obliged to comply with the DPA and other relevant laws and regulations and that the marketing organisation only carries out the instructions given to it by the retailer. A named individual in the marketing organisation should be accountable for ensuring that these instructions are followed. The marketing organisation will have no separate rights over the personal data collected on behalf of the retailer.

**Visibility**
The responsible person should ensure full information is provided to the individual before any collection of their personal data takes place. The responsible person must also ensure that the purpose(s) for which the personal data is required are clearly stated at all points of collection and that the data being collected is consistent with these purposes and not excessive.

If the organisation wishes to use the personal data for another purpose, the responsible person should ensure that this is on the basis of the individual’s agreement or another lawful condition - not part of the default terms and conditions or buried in the small print. The responsible person should ensure that the purposes state if the personal data is likely to be shared with any third party and whether this is optional.

**Consent**
The responsible person must ensure that their area of the organisation either secures the consent of data subjects before storing and/or accessing personal data or makes it clear before collection why consent is not needed. They should also ensure that they have consent to share with third parties if they intend to do so (other than where they are legally obliged to pass on personal data). At the time of collection personal data that is essential to the primary purpose must be clearly distinguished from personal data that is not essential and accordingly optional.

**Example 23:** A high street retailer needs credit card details in order to process a purchase. They may ask for contact details because they want to add the customer to their marketing database, but the retailer’s staff must make it clear that these details are optional and are for the secondary purpose of marketing.

**Access**
The responsible person must ensure that appropriate physical, personnel and electronic controls and management processes are in place to protect and secure access to all personal data in their custody from external attack, interference, internal abuse or carelessness. This is also the responsibility of any third party offering a service.

**Stewardship**
The responsible person must ensure that any personal data collected is the minimum needed, and is only used for the stated purpose(s). The responsible person should ensure that any personal data held has properties such as checks on accuracy and retention time or a relevant expiry date associated with it. The integrity of personal data must be maintained throughout the data lifespan. A risk assessment of the data held should be carried out from the time of collection. This assessment should be associated with the data throughout the data lifespan.

If the organisation has obtained consent to share personal data with any third party, the responsible person should ensure that the third party understands both the risks associated with the data that it will hold and any caveats associated with its integrity.

The responsible person should ensure that when the organisation passes on personal data they have also passed on their obligation to protect that data throughout any community of sharing.

There should be an onus on the responsible person within a social networking organisation to manage the extent to which free-format input by data subjects to blogs and forums is published with attributions and to make the extent of publication clear to data subjects at the point of sign up.
Duties of the responsible person

Use - primary use, maintenance, updates, back-up and sharing

**Accountability**
The responsible person must ensure that all the data handlers are aware of their overall responsibility for compliance with the DPA.
The responsible person must also ensure that the data handlers are adequately trained and comply with the procedures and standards for handling personal data that are specified in the organisation.

**Visibility**
The responsible person should ensure that an audit trail of all accesses to personal data is maintained and examined periodically.

**Consent**
Where there is no legal obligation to share personal data, the responsible person should check that consent has been obtained from the data subject before passing it on to a third party. If the organisation wishes to use data for a secondary purpose for which consent was not obtained at the time of data collection, then the data subject must be informed of this and their consent to such use obtained, unless some other legal condition is being met. The responsible person must ensure that effective and timely processes are in place for dealing with data subject enquiries relating to their personal data and also for dealing with requests for data corrections, removals or cessation of particular processes.

**Example 24:** A customer requests that a retailer stops processing their data. The responsible person must ensure that no further use is made of this customer data other than that required to meet financial or other legal requirements and that the customer is so advised.

**Access**
The responsible person must ensure that:
- appropriate operating procedures and security control mechanisms, including access logging, are in place to prevent unauthorised access to personal data;
- the integrity and sustainability of the personal data that is held are maintained by regular updates, back-ups, appropriate data matching procedures and adequately secure storage conditions.

**Stewardship**
The responsible person should regularly review the business processes and personal data holdings to ensure that the scope, accuracy and currency of that personal data are maintained. The responsible person needs to ensure that personal data errors pointed out by the data subject or otherwise identified are actioned and that any queries and complaints are recorded. It may also be necessary to inform third parties with whom the personal data have been shared. The responsible person should also ensure that any data breaches are dealt with appropriately and that data subjects are informed if their privacy has been compromised.

**Example 25:** When a customer queries the accuracy of their credit record, this query must be noted and passed onto the records of any credit reference agencies to which the original data was passed. When the query is resolved then the records held by the organisation giving credit and the credit reference agency must be updated.

Output - subsequent use, copying, reuse, exporting and disposal

**Accountability**
The responsible person must ensure that personal data:
- covered by a documented data retention policy that reflects the valid purposes, the nature of the data and any legal requirements, and that this information is available to the individual whose data is being kept;
- disposed of securely in accordance with the data retention policy.

**Visibility**
The responsible person should maintain an accurate record of what personal data was shared with third parties and why. The responsible person should also maintain a record of archives and disposals.

**Consent**
The responsible person should seek approval from data subjects if all or part of their personal data is to be passed to a third party not previously identified, unless the organisation is bound by a legal obligation or can rely on another lawful condition.

**Access**
The responsible person must ensure that no one within the organisation or any third party has access to personal data without the appropriate authority to do so.

**Stewardship**
The responsible person should ensure that:
- any caveats relating to the personal data at the time of collection are linked to the data throughout any sharing process and the boundaries of stewardship and ownership of risks are made explicit to all parties;
- personal data no longer required to support the business process is securely and legally disposed of in accordance with a documented data retention policy;
- contracts are in place with any third parties used in storage or disposal of personal data, and audits are carried out to ensure the contract requirements are met.
**Responsibilities of the data handler**

Data handlers are the people in organisations who are authorised to handle personal data. As an individual handling personal data, you need to know who, in your organisation, is accountable (for example a board member) and to whom the board has delegated aspects of accountability (the responsible person) for that personal data and exactly what you, as an individual data handler, have been authorised to do with that data. That authorisation should be in writing and not an ‘informal’ arrangement or request. You should never exceed your authorisation and should query anyone who asks you to exceed it. Data handlers should always maintain high ethical standards when processing personal data.

**Input– collection, verification and cleansing**

- **Accountability**
  Authorised personal data handlers are accountable to the responsible person in their organisation for the accurate collection and transcription of personal data from the data subject.

- **Visibility**
  Data handlers should maintain high ethical standards when accessing personal data. Where information is being collected directly from the data subject the data handler should always be able to say for whom the information is being collected, why it is needed and who else the data subject should contact in the case of a query. The data handler must be given sufficient training and information to do this.

- **Consent**
  Data handlers tasked with the collection of personal data should verify that, where relevant, the consent of the data subject has been obtained for the personal data collected. Data subjects are entitled at any time to raise questions or objections to their data being collected.

Data handlers should be given clear instructions to follow should they receive any objections from the data subject. Data handlers should always be able to distinguish clearly between mandatory and optional data gathering.

- **Access**
  Data handlers should only collect and store the essential personal data required by the organisation for the purpose(s) stated and as required by the organisation.

- **Stewardship**
  Data handlers have a duty of care with respect to the personal data they handle to ensure that its integrity is maintained. They should ensure the security of personal data from the time it is collected up to the point where their responsibility ceases.
Responsibilities of the data handler

Use - primary use, maintenance, updates, back-ups and sharing

**Accountability**
Data handlers should ensure that they only access personal data in strict accordance with legitimate business needs within their delegated authority. They must at all times follow all relevant policies and procedures. Should a data handler diverge from any of these, they risk breaching the law and consequent legal action against them or their organisation.

**Visibility**
Data handlers should ensure that all of their actions can be justified and audited.

**Consent**
Data handlers should ensure that they have the relevant authorisation from the responsible person prior to using and/or sharing personal data.

**Access**
Data handlers should only access personal data when they have a legitimate reason and authority to do so, and should ensure that the integrity and accuracy of the personal data are maintained during transit and sharing.

**Stewardship**
Data handlers should report and, where possible, resolve or correct inconsistencies and/or errors in the integrity and accuracy of personal data. Data handlers should report any suspected data breaches to the responsible person.

Output - subsequent use, copying, reuse, exporting and disposal

**Accountability**
Data handlers should ensure that anyone requesting access to, or copies of, personal data is authorised to receive it.

**Visibility**
Data handlers should maintain records of any transfer, correction or disposal of personal data.

**Consent**
Data handlers should ensure that they have authorisation from the responsible person to reuse, share or export personal data.

**Access**
Data handlers should only copy or pass on personal data when they have a legitimate reason and the authority to do so.

**Stewardship**
Data handlers should ensure that, if personal data is to be sent to a third party either electronically, via removable electronic media or on paper, the data is encrypted or otherwise protected in a manner appropriate to its sensitivity and accompanied by specific instructions clearly relating to any caveats about or restrictions on access or use.

‘You should never exceed your authorisation and should query anyone who asks you to exceed it.’
PERSONAL DATA GUARDIANSHIP CODE

What you can do about your personal information

Our personal information (personal data) is held by many organisations. In legal terms this means that we are all data subjects (see ‘What is personal data?’)

Protecting your personal data

When personal data goes missing, is (mis)used for unexpected purposes or falls into the wrong hands, it can be embarrassing, costly and emotionally draining for those involved. You have the right to expect organisations to handle your information lawfully, but there are also a series of things that you can do to protect your information:

• Think before sharing your (or anybody else’s) personal information. And think again...

• Never ever give out your bank account or password information when the conversation was not initiated by you. Your bank will never ask for your PIN and your IT department will never ask for your password.

• Do not respond to suspicious emails or unexpected text messages from people you do not know.

• Only share information that is clearly needed by an organisation for them to fulfil their part of the transaction.

• If you don’t understand why particular personal information is being asked for, be prepared to query or refuse the request.

• Take particular care with social networking sites where your personal data might be seen by countless others.

• If you don’t want to receive marketing messages, faxes or junk mail, register with the Telephone Preference Service, Fax Preference Service and Mail Preference Service.

• Visit Get Safe Online and follow its advice.

What are your rights?

Under the law you have the right to:

• obtain a copy of all of the information that an organisation holds about you. In some cases, you may need to pay a nominal fee to the organisation to receive it;

• have incorrect, misleading or out-of-date information about you corrected or at least a notice of correction applied to your file;

• know whether an organisation or someone acting on their behalf is using your personal information;

• know what information is being used and why and to whom it may be disclosed or shared;

• know from where an organisation received its information about you;

• object to processing of your personal data;

• ask that the organisation no longer retains your personal data;

• choose not to receive direct marketing information by post, email or SMS. If you didn’t make this choice clear when your contact information was initially collected, you can request this by writing to the organisation concerned.

These rights may be limited in specific cases by exemptions that are detailed in the law.

What can you do when it goes wrong?

If you think an organisation may have breached the Data Protection Act in the way it holds and handles your personal data or information, you should firstly contact the organisation. If you do not obtain satisfaction, complain to the Information Commissioner’s Office.

For advice on how to complain, visit the Information Commissioner’s website www.ico.org.uk or phone their helpline on 0303 123 1113.

The Information Commissioner’s Office website also contains a personal information toolkit and other resources to assist in raising awareness of the rights of data subjects.