Guide to data protection for Organisations as detailed in by the ICO.
https://ico.org.uk/for-organisations/guide-to-data-protection/

A. KEY DEFINITIONS

Data - Definitions

What type of information is protected by the Data Protection Act?

The Act regulates the use of "personal data". To understand what personal data means, we need to first look at how the Act defines the word "data".

Data means information which –
(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
(b) is recorded with the intention that it should be processed by means of such equipment,
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or
(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

Paragraphs (a) and (b) make it clear that information that is held on computer, or is intended to be held on computer, is data. So data is also information recorded on paper if you intend to put it on computer.

What is Personal Data?

Personal data means data which relate to a living individual who can be identified –
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be "personal data".

What activities are regulated by the Data Protection Act?
The Act regulates the "processing" of personal data.

Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –
(a) organisation, adaptation or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
(d) alignment, combination, blocking, erasure or destruction of the information or data.
The definition of processing is very wide and it is difficult to think of anything an organisation might do with data that will not be processing.

Who has rights and obligations under the Data Protection Act?

This guide describes how the Act protects the rights of individuals whom the data is about (data subjects), mainly by placing duties on those who decide how and why such data is processed (data controllers). We generally use the terms "organisation" and "you" rather than "data controller", and "individual" instead of "data subject".

However, it is important to understand:
- what these terms mean and their significance; and
- the difference between a data controller and a data processor, as they are treated differently under the Act.

Data subject means an individual who is the subject of personal data.
In other words, the data subject is the individual whom particular personal data is about. The Act does not count as a data subject an individual who has died or who cannot be identified or distinguished from others.

Data controller means … a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

A data controller must be a "person" recognised in law, that is to say:

- individuals;
- organisations; and
- other corporate and unincorporated bodies of persons.

Data controllers will usually be organisations, but can be individuals, for example self-employed consultants. Even if an individual is given responsibility for data protection in an organisation, they will be acting on behalf of the organisation, which will be the data controller.

In relation to data controllers, the term jointly is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term in common applies where two or more persons share a pool of personal data that they process independently of each other.

Data controllers must ensure that any processing of personal data for which they are responsible complies with the Act. Failure to do so risks enforcement action, even prosecution, and compensation claims from individuals.

Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data processors are not directly subject to the Act. However, most data processors, if not all, will be data controllers in their own right for the processing they do for their own administrative purposes, such as employee administration or sales.

Data controllers remain responsible for ensuring their processing complies with the Act, whether they do it in-house or engage a data processor. Where roles and responsibilities are unclear, they will need to be clarified to ensure that personal data is processed in accordance with the data protection principles. For these reasons organisations should choose data processors carefully and have in place effective means of monitoring, reviewing and auditing their processing.

Who determines the "purpose and manner" of processing?

A person is only a data controller if, alone or with others, they "determine the purposes for which and the manner in which any personal data are processed". In essence, this means that the data controller is the person who decides how

and why personal data is processed. However, we take the view that having some discretion about the smaller details of implementing data processing (ie the manner of processing) does not make a person a data controller.

What about processing that is required by law?
The Data Protection Act says:

Where personal data are processed only for purposes for which they are required by or under any enactment to be processed, the person on whom the obligation to process the data is imposed by or under that enactment is for the purposes of this Act the data controller.
Our view is that this provision applies wherever there is a statutory duty that involves the publication or use of personal data. We do not think that it should be interpreted more narrowly – as applying only where there is an express statutory duty to process personal data – because obligations imposed by legislation other than the Data Protection Act do not usually refer to processing personal data.
So, if performing a legal duty necessarily involves processing personal data, the person required to process such data will be the data controller and will be legally responsible for ensuring that the processing complies with the Act.

This is the case even if processing personal data is an inevitable, but not the main, part of performing the legal duty. If performing a legal duty directly or indirectly involves processing personal data, the organisation under the duty will be the data controller in relation to such data processing.
Sometimes, an organisation is subject to a duty that requires processing personal data, but delegates its performance to another person. In these circumstances the person with the overall responsibility for achieving the purpose, or performing the function, bears the responsibilities of the data controller. We place greatest weight on purpose rather than manner of processing – identifying whose decision to achieve a business purpose (or to carry out a statutory function) has led to personal data being processed.

How long do data protection rights and duties last?

Your duties under the Act apply throughout the period when you are processing personal data – as do the rights of individuals in respect of that personal data. So you must comply with the Act from the moment you obtain the data until the time when the data has been returned, deleted or destroyed. Your duties extend to the way you dispose of personal data when you no longer need to keep it – you must dispose of the data securely and in a way which does not prejudice the interests of the individuals concerned.

Changes in an organisation's circumstances do not reduce an individual's rights under the Act. Even if an organisation goes out of business, individuals are still entitled to expect that their personal data will be processed in accordance with the data protection principles. However, responsibility for ensuring this happens may shift, depending on the circumstances.

What are the other key definitions in the Data Protection Act?
Most of the concepts explained above are defined in section 1 of the Data Protection Act. However, there are other important definitions. In particular, section 70 sets out supplementary definitions and section 71 lists provisions defining or explaining expressions used in the Act. The following is a list of some of the other defined terms used in the Act.
Inaccurate data. The Act states:

For the purposes of this Act data are inaccurate if they are incorrect or misleading as to any matter of fact.
Personal data may not be inaccurate if it faithfully represents someone's opinion about an individual, even if the opinion proves incorrect (for example, a doctor's medical opinion about an individual's condition). In these circumstances, the data would not need to be "corrected", but the data controller may have to add a note stating that the data subject disagrees with the opinion.
Recipient. The Act states:

Recipient, in relation to personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.
The Act provides that a data controller's notification of processing must include "a description of any recipient or recipients to whom the data controller intends or may wish to disclose the data". Data controllers must therefore provide a description of possible recipients, including employees, agents and data processors, rather than a specific list of actual recipients.

The Act also provides that an individual making a subject access request is entitled to be given "a description of the recipients or classes of recipients to whom [personal data] are or may be disclosed". This is so that individuals can have a better understanding of what is done with their personal data. However, the definition of "recipient" goes on to say, in effect, that people need not be identified as recipients just because information is disclosed to them as part of an

inquiry they have legal power to make. This is to prevent an official investigation being compromised if an individual making a subject access request is tipped off that an investigation is or soon will be under way – such as a police, customs or trading standards investigation.

Third party, in relation to personal data, means any person other than –
(a) the data subject,
(b) the data controller, or
(c) any data processor or other person authorised to process data for the data controller or processor.
The usual meaning of the term "third party" is someone other than the two main parties involved, for example someone other than the husband and wife in divorce proceedings. In relation to data protection, the main reason for this particular definition is to ensure that a person such as a data processor, who is effectively acting as the data controller, is not considered a third party
Although a data controller's employee to whom information is disclosed will be a "recipient", they will usually not be a "third party". This is because the employee will usually be acting in their employment capacity, and so will be acting on behalf of the data controller. If a data controller's employee receives personal data from their employer outside the normal course of their employment, the employee will be a third party in relation to their employer.

Example
A data controller may decide to disclose to one of its employees (Tom) personal data relating to another of its employees (Dick), for Tom to use as evidence in possible legal action (unconnected with Tom's employment). In this situation, Tom is not receiving the information in the course of his employment with the data controller, so will be a third party.
The term "third party" is used in the Data Protection Act relating to accuracy; to "fair processing"; and in two of the conditions for processing. Although the term "third party" is not used in the Act's provisions about subject access, further information can be found by reading the (pdf) and the section of this guide on Subject access request: In brief – what is an individual entitled to?

B. Data protection principles

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
(a) at least one of the conditions in Schedule 2 is met, and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Personal data shall be accurate and, where necessary, kept up to date.

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Personal data shall be processed in accordance with the rights of data subjects under this Act.

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.

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Principle 1 - Fair and Lawful

The Data Protection Act requires you to process personal data fairly and lawfully. This section explains how to comply with this requirement, and gives examples of good practice in handling personal data.
The requirement to process personal data fairly and lawfully is set out in the first data protection principle and is one of eight such principles at the heart of data protection. The main purpose of these principles is to protect the interests of

the individuals whose personal data is being processed. They apply to everything you do with personal data, except where you are entitled to an exemption.
So the key to complying with the Data Protection Act is to follow the eight data protection principles.
Later sections of the guide deal with the other data protection principles in more detail.

In brief – what does the Data Protection Act say about handling personal data fairly and lawfully?

The Data Protection Act says that:

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
(a) at least one of the conditions in Schedule 2 is met, and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

This is the first data protection principle. In practice, it means that you must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure you do not do anything unlawful with the data.

Principle 2 - Purposes

Other sections of this guide explain that you may only process personal data if you have a legitimate basis for doing so, and that any processing must be fair and lawful. This section explains the Data Protection Act's additional requirement that you specify the purpose or purposes for which you obtain personal data, and that anything you do with the data must be compatible with this (or, as the Data Protection Act says, "not … in any manner incompatible" with it.)

In brief – what does the Data Protection Act say about specifying the purposes for which personal data is processed?

The Data Protection Act says that:

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

This requirement (the second data protection principle) aims to ensure that organisations are open about their reasons for obtaining personal data, and that what they do with the information is in line with the reasonable expectations of the individuals concerned.
There are clear links with other data protection principles – in particular the first principle, which requires personal data to be processed fairly and lawfully. If you obtain personal data for an unlawful purpose, for example, you will be in breach of both the first data protection principle and this one. However, if you comply with your obligations under the other data protection principles, you are also likely to comply with this principle, or at least you will not do anything that harms individuals.
In practice, the second data protection principle means that you must:

- be clear from the outset about why you are collecting personal data and what you intend to do with it;
- comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;
- comply with what the Act says about notifying the Information Commissioner; and
- ensure that if you wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

Principle 3 - Adequacy

The Data Protection Act requires you to ensure you only collect the personal data you need for the purposes you have specified. You are also required to ensure that the personal data you collect is sufficient for the purpose for which it was collected.
These requirements of data adequacy and data minimisation are covered by principle 3 of the Data Protection Act. It is the first of three principles, along with principles 4 and 5, covering information standards.

In brief – what does the Data Protection Act say about the amount of personal data you may hold?

The Act says that:
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
This is the third data protection principle. In practice, it means you should ensure that:

- you hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual; and
- you do not hold more information than you need for that purpose.

So you should identify the minimum amount of personal data you need to properly fulfil your purpose. You should hold that much information, but no more. This is part of the practice known as "data minimisation".

Principle 4 - Accuracy

The second of the principles covering information standards, principle 4 covers the accuracy of personal data. The Data Protection Act imposes obligations on you to ensure the accuracy of the personal data you process. It must also be kept up to date where necessary.

This requirement is closely linked with the requirement under principle 3 that personal data is adequate. Ensuring the accuracy of personal data will assist you in complying with this requirement as well.

In brief – what does the Data Protection Act say about accuracy and updating?

The Act says that:
Personal data shall be accurate and, where necessary, kept up to date.
This is the fourth data protection principle. Although this principle sounds straightforward, the law recognises that it may not be practical to double-check the accuracy of every item of personal data you receive. So the Act makes special provision about the accuracy of information that individuals provide about themselves, or that is obtained from third parties.
To comply with these provisions you should:

- take reasonable steps to ensure the accuracy of any personal data you obtain;
- ensure that the source of any personal data is clear;

- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to update the information.

Principle 5 - Retention

What does the Data Protection Act say about keeping personal data?

The Act does not set out any specific minimum or maximum periods for retaining personal data. Instead, it says that: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
This is the fifth data protection principle. In practice, it means that you will need to:

- review the length of time you keep personal data;
- consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date.

Principle 6 - Rights

The Data Protection Act gives rights to individuals in respect of the personal data that organisations hold about them. The Act says that:

"Personal data shall be processed in accordance with the rights of data subjects under this Act."

This is the sixth data protection principle, and the rights of individuals that it refers to are:

- a right of access to a copy of the information comprised in their personal data;
- a right to object to processing that is likely to cause or is causing damage or distress;
- a right to prevent processing for direct marketing;
- a right to object to decisions being taken by automated means;
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to claim compensation for damages caused by a breach of the Act.

This part of the guide explains these rights, sets out the duties of organisations in this regard and gives examples of good practice.

Subject Access request.

In brief – what is an individual entitled to?
This right, commonly referred to as subject access, is created by section 7 of the Data Protection Act. It is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this, and an individual who makes a written request and pays a fee is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the information comprising the data; and given details of the source of the data (where this is available).

An individual can also request information about the reasoning behind any automated decisions, such as a computer-generated decision to grant or deny credit, or an assessment of performance at work (except where this information is a trade secret). Other rights relating to these types of decisions are dealt with in more detail in Automated decision taking.
In most cases you must respond to a subject access request promptly and in any event within 40 calendar days of receiving it. However, some types of personal data are exempt from the right of subject access and so cannot be obtained by making a subject access request. For more information, please see Exemptions.

Damage or distress.

In brief – what does the Data Protection Act say about objecting to processing?

The Act refers to the "right to prevent processing". Although this may give the impression that an individual can simply demand that an organisation stops processing personal data about them, or stops processing it in a particular way, the right is often overstated. In practice, it is much more limited. An individual has a right to object to processing only if it causes unwarranted and substantial damage or distress. If it does, they have the right to require an organisation to stop (or not to begin) the processing in question.

So, in certain limited circumstances, you must comply with such a requirement. In other circumstances, you must only explain to the individual why you do not have to do so.

In more detail…

How can an individual prevent me processing their personal data?

An individual who wants to exercise this right has to put their objection in writing to you and state what they require you to do to avoid causing damage or distress. We refer to this notice as an "objection to processing" although it is also known as a "section 10 notice" in practice. The Act limits the extent to which you must comply with such an objection, in the following ways:

- an individual can only object to you processing their own personal data;
- processing an individual's personal data must be causing unwarranted and substantial damage or distress; and
- the objection must specify why the processing has this effect.

In addition, an individual has no right to object to processing if:

- they have consented to the processing;
- the processing is necessary:
  - in relation to a contract that the individual has entered into; or
  - because the individual has asked for something to be done so they can enter into a contract;
- the processing is necessary because of a legal obligation that applies to you (other than a contractual obligation); or
- the processing is necessary to protect the individual's "vital interests".

<u>Preventing Direct Marketing.</u>

In brief – what does the Data Protection Act say about direct marketing?
Individuals have the right to prevent their personal data being processed for direct marketing. An individual can, at any time, give you written notice to stop (or not begin) using their personal data for direct marketing. Any individual can exercise this right, and if you receive a notice you must comply within a reasonable period.

Automated Decision Taking.

In brief – what does the Data Protection Act say about automated decision taking?

The right of subject access allows an individual access to information about the reasoning behind any decisions taken by automated means. The Act complements this provision by including rights that relate to automated decision taking. Consequently:

- an individual can give written notice requiring you not to take any automated decisions using their personal data;
- even if they have not given notice, an individual should be informed when such a decision has been taken; and
- an individual can ask you to reconsider a decision taken by automated means.

These rights can be seen as safeguards against the risk that a potentially damaging decision is taken without human intervention. We explain below what is meant by automated decision taking and how the rights work in practice.
The number of organisations who take significant decisions about individuals by wholly automated means is relatively small – there is often some human intervention in making the decisions. However, it is sensible to identify whether any of the operations you perform on personal data constitute "automated decisions". This will help you decide whether you need to have procedures to deal with the rights of individuals in these cases.

Correcting inaccurate personal data.

In brief – what does the Data Protection Act say about rights to correct or delete inaccurate information?

The fourth data protection principle requires personal data to be accurate (see Keeping personal data accurate and up to date). Where it is inaccurate, the individual concerned has a right to apply to the court for an order to rectify, block, erase or destroy the inaccurate information. In addition, where an individual has suffered damage in circumstances that would result in compensation being awarded and there is a substantial risk of another breach, then the court may make a similar order in respect of the personal data in question.

Compensation.

In brief – what does the Data Protection Act say about the right to compensation?

If an individual suffers damage because you have breached the Act, they are entitled to claim compensation from you. This right can only be enforced through the courts. The Act allows you to defend a claim for compensation on the basis that you took all reasonable care in the circumstances to avoid the breach.

Principle 7 - Security

This part of the guide offers an overview of what the Data Protection Act requires in terms of security, and aims to help you decide how to manage the security of the personal data you hold. We cannot provide a complete guide to all aspects of security in all circumstances and for all organisations, but this part identifies the main points. We also provide details of other sources of advice and information about security.
There is no "one size fits all" solution to information security. The security measures that are appropriate for an organisation will depend on its circumstances, so you should adopt a risk-based approach to deciding what level of security you need.

In brief – what does the Data Protection Act say about information security?

The Data Protection Act says that:

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 is the seventh data protection principle. In practice, it means you must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. In particular, you will need to:

- design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach;
- be clear about who in your organisation is responsible for ensuring information security;
- make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively.

Principle 8 - International

This section provides practical advice to companies or other organisations who want to send personal data outside the European Economic Area (EEA).

In brief – what does the Data Protection Act say about sending personal data outside the EEA?
The Data Protection Act says that:

Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
This is the eighth data protection principle, but other principles of the Act will also usually be relevant to sending personal data overseas. For example, the first principle (relating to fair and lawful processing) will in most cases require you to inform individuals about disclosures of their personal data to third parties overseas. The seventh principle (concerning information security) will also be relevant to how the information is sent and the necessity to have contracts in place when using sub-contractors abroad.

The Act also sets out the situations where the eighth principle does not apply, and these situations are also considered in more detail in this section.

If you are considering sending personal data outside the EEA, work through the following checklist to help you decide if the eighth principle applies and, if so, how to comply with it to make a transfer.

1. Do you need to transfer personal data abroad?
Can you achieve your objectives without processing personal data at all? For example, could the information be anonymised?
2. Are you transferring the data to a country outside the EEA or will it just be in transit through a non-EEA country?
If data is only in transit through a non-EEA country, there is no transfer outside the EEA. Note that if you add personal data to a website based in the EU that is accessed in a country outside the EEA, there will be a transfer of data outside the EEA.
3. Have you complied with all the other data protection principles?

If you transfer personal data outside the EEA, you are required to comply with all the principles and the Act as a whole, not just the eighth principle relating to international data transfers.
4. Is the transfer to a country outside the EEA?
There are no restrictions on the transfer of personal data to EEA countries.
5. Is the transfer to a country on the EU Commission's list of countries or territories providing adequate protection for the rights and freedoms of data subjects in connection with the processing of their personal data?
Transfers may be made to any country or territory in respect of which the Commission has made a 'positive finding of adequacy'.
6. If the transfer is to the United States of America, has the US recipient of the data provided adequate protection for the transfer of personal data?
For the latest information on the transfer of personal data to the USA please see our guidance on using the privacy shield to transfer data to the US.

Conditions for Processing.

This section explains the conditions that need to be satisfied before you may process personal data.

In brief – what does the Data Protection Act say about the "conditions for processing"?

The first data protection principle requires, among other things, that you must be able to satisfy one or more "conditions for processing" in relation to your processing of personal data. Many (but not all) of these conditions relate to the purpose or purposes for which you intend to use the information.
The conditions for processing take account of the nature of the personal data in question. The conditions that need to be met are more exacting when the information being processed is sensitive personal data, such as information about an individual's health or criminal record.
However, our view is that in determining if you have a legitimate reason for processing personal data, the best approach is to focus on whether what you intend to do is fair. If it is, then you are very likely to identify a condition for processing that fits your purpose.
Being able to satisfy a condition for processing will not on its own guarantee that the processing is fair and lawful – fairness and legality must still be looked at separately. So it makes sense to ensure that what you want to do with personal data is fair and lawful before worrying about the conditions for processing set out in the Act.

Exemptions.

In brief – are there any exemptions from the Data Protection Act?

The rights and duties set out in the Data Protection Act are designed to apply generally, but there are some exemptions from the Act to accommodate special circumstances. The exemptions tend to use complex language and, while this chapter has tried to clarify matters, it has had to use some of the same language so as not to mislead.
If an exemption applies, then (depending on the circumstances) you will be exempt from the requirement:

- to register with the ICO (to "notify"); and/or
- to grant subject access to personal data; and/or
- to give privacy notices; and/or
- not to disclose personal data to third parties.

Entitlement to an exemption depends in part on your purpose for processing the personal data in question – for example, there is an exemption from some of the Act's requirements about disclosure and non-disclosure that applies to processing personal data for purposes relating to criminal justice and taxation. However, you must consider each exemption on a case-by-case basis because the exemptions only permit you to depart from the Act's general requirements to the minimum extent necessary to protect the particular functions or activities the exemptions concern.

Complaints.

What happens when someone complains?

If a member of the public is concerned about your information rights practices, we believe that you, as the organisation responsible, should deal with it.
We expect you to respond to any information rights concerns you receive, clarifying how you have processed the individual's personal information in that case and explaining how you will put right anything that's gone wrong.
If a member of the public has engaged with you but is still dissatisfied, they may report their concern to the ICO.

Anonymisation.

What is anonymisation?

Anonymisation is the process of turning data into a form which does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information. The Data Protection Act controls how organisations use 'personal data' – that is, information which allows individuals to be identified.
Organisations are increasingly reliant on anonymisation techniques to enable wider use of personal data. The code of practice explains the issues surrounding the anonymisation of personal data, and the disclosure of data once it has been anonymised. The code describes the steps an organisation can take to ensure that anonymisation is conducted effectively, while retaining useful data.

For further information consult the guide: https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

Big Data

Big data, artificial intelligence (AI) and machine learning are becoming widespread in the public and private sectors. Data is being collected from an increasing variety of sources and the analytics being applied are more and more complex. While many benefits flow from these types of processing operations, when personal data is involved there are implications for privacy and data protection.
In our view though, these implications are not barriers. There are several tools and approaches that not only assist with data protection compliance but also encourage creativity, innovation, and help to ensure data quality. So it's not big data *or* data protection, it's big data **and** data protection. The benefits of big data, AI and machine learning will be sustained by upholding key data protection principles and safeguards.

For further information consult the guide: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

Data Sharing

The data sharing code of practice is a statutory code which has been issued after being approved by the Secretary of State and laid before Parliament. The code explains how the Data Protection Act applies to the sharing of personal data.

It provides practical advice to all organisations, whether public, private or third sector, that share personal data and covers systematic data sharing arrangements as well as ad hoc or one off requests to share personal data.
Adopting the good practice recommendations in the code will help organisations to collect and share personal data in a way that complies with the law, is fair, transparent and in line with the rights and expectations of the people whose data is being shared.
For further information consult the guide: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

Employment

As an employer, you have responsibilities to ensure your employees' personal details are respected and properly protected.

For further information consult the guide: https://ico.org.uk/media/for-organisations/documents/1128/quick_guide_to_the_employment_practices_code.pdf

Online and apps

Personal information online
More and more people are conducting their personal affairs online. Online shopping, social networking, job hunting and the ability to carry out 'official' functions, such as renewing car tax or contacting local councils and government departments online, are now an everyday part of life.

For further information consult the guide: https://ico.org.uk/media/for-organisations/documents/1591/personal_information_online_cop.pdf

Privacy by Design

What is 'privacy by design'?
Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. Unfortunately, these issues are often bolted on as an after-thought or ignored altogether.

Although this approach is not a requirement of the Data Protection Act, it will help organisations comply with their obligations under the legislation.
The ICO encourages organisations to ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle. For example when:

- building new IT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes.

We would like to see more organisations integrating core privacy considerations into existing project management and risk management methodologies and policies.

For further information consult the guide: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf