babcock™

Legislation – Information and Data

This is about the legislation relating to the use and storage of information and data. These laws have been arranged in alphabetical order for ease of use.

Companies Act 2006

C

The Companies Act 2006 is the main piece of legislation which governs company law in the UK. It is the longest piece of legislation ever enacted in the UK, with over 1,300 sections. Following eight years of consultation, the final provisions of the Act became law in October 2009.

The prime aims of the Act are to modernise and simplify company law, to codify directors' duties, to grant improved rights to shareholders, and to simplify the administrative burden carried by UK companies.

- The incorporation process for new companies has been simplified.
- Many company duties and submissions can now be fulfilled electronically, as can communications with shareholders.
- Company directors' duties have been codified for the first time, including an obligation to promote the success of the company, to consider the community and the environment, the interests of employees, and to be fair to shareholders.
- Indirect shareholders have more rights, including the right to sue the company's director(s) if fraud or negligence is suspected.
- Nominee shareholders can elect to receive company information electronically if they wish.
- Limited companies are no longer required to have a company secretary, and can be run by one director.

- The company naming rules have been upgraded.
- Company directors can now provide a service address, in order to keep their residential address off the public record.
- Companies can use new 'model' Articles of Association, provided by Companies House.
- Private companies are no longer obliged to hold an Annual General Meeting (AGM).
- The share capital rules have been simplified for private companies.
- The legislation supersedes the Companies Act 1985.

Common Law Duty of Confidentiality

Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges; hence, it is also referred to as 'judge-made' or case law. The law is applied by reference to those previous cases, so common law is also said to be based on precedent.

The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent.

Three circumstances making disclosure of confidential information lawful are:

- Where the individual to whom the information relates has consented.
- Where disclosure is necessary to safeguard the individual, or others, or is in the public interest.
- Where there is a legal duty to do so, for example a court order.

Copyright, Designs and Patents Act 1988

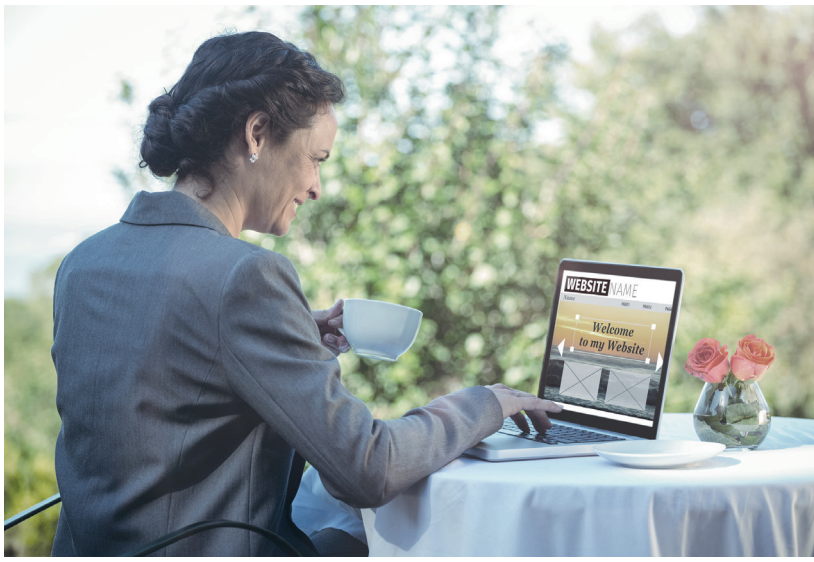
This legislation relates to the work of others and its use. Artworks, music, designs, documentation etc. are all subject to copyright law. Permission must be obtained from the author before it can be used by another person.

F

The Freedom of Information Act 2000

The Freedom of Information Act came into force in January 2005. It gives the public a right of access to all kinds of recorded information held by the government and local authorities. There are some exemptions to that right, if there is a good reason (in the public interest). If this is the case, the public authority must tell you why they have withheld information.

You will be able to access information for example if you want to check what a local authority is doing to tackle a problem and the reasons for their decisions or to find out about their spending.



If you ask for information about yourself, then your request will be handled under the Data Protection Act. You will normally receive a reply within 20 days.

The Act applies to public bodies including:

- Government departments and local assemblies.
- Local authorities and councils.
- Health trusts, hospitals and doctors' surgeries.
- Schools, colleges and universities.
- Publicly funded museums.
- The Police.
- Non-departmental public bodies, committees and advisory bodies.

G

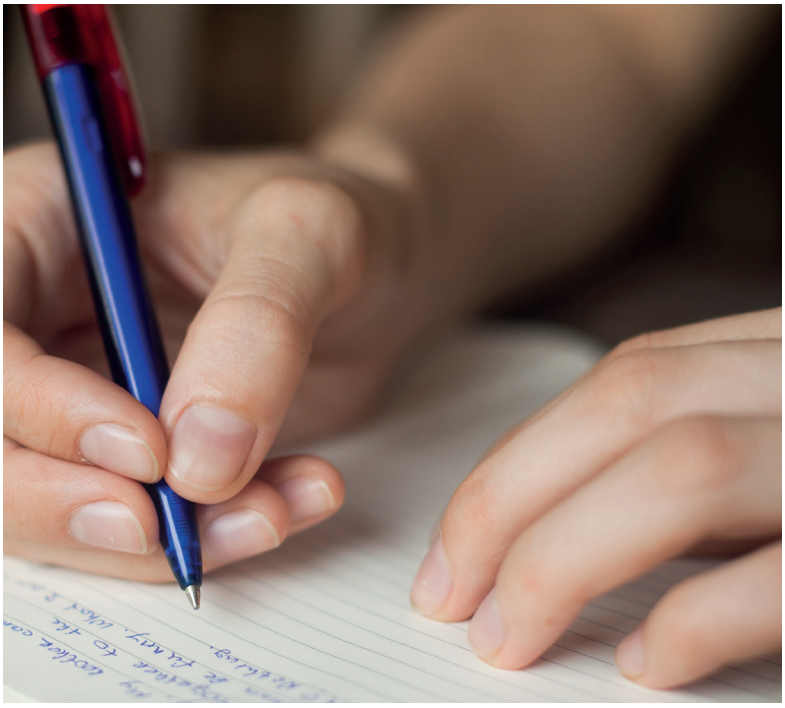
General Data Protection Regulations (GDPR)

On the 25th May 2018, the current Data Protection Act (DPA) was replaced by the EU General Data Protection Regulations (GDPR). Processing data can be automated or manual, and may be carried out by organisations operating within the EU and/or organisations outside the EU that offer goods or services to individuals in the EU.

Data Controller and Processor Legal Responsibilities

- Data Subject – the person the data is about.
- Data Controller – the person or organisation which determines the reason for processing personal data.
- Data Processor – a person or organisation which processes personal data on behalf of the controller.

Data Processors' legal responsibilities have increased. Previously the onus was on the Data Controller to select a suitable Processor and if they didn't legal responsibility fell to the Controller but now the Controller and Processor have very similar responsibilities.



Processors have specific legal obligations; for example, to maintain records of personal data and processing activities. They also have a significant legal liability if they are responsible for a breach.

However, Controllers are not relieved of their obligations where a Processor is involved; obligations are placed on Controllers to ensure their contracts with Processors comply with the legislation.

Personal and Personal Sensitive Data -– now known as Special Categories of Data

The definition of what constitutes Personal Data (information about a person -'data subject) is changing and will now include online identifiers, e.g. IP addresses.

Personal Sensitive Data will now be known as Special Categories of Data; and again the definition of these special categories has changed and now includes biometric and genetic information but excludes criminal convictions and offences.

These special categories are retained:

a. Racial or ethnic origin.
b. Political opinion.
c. Religious beliefs or other beliefs of a similar nature.
d. Whether they are a member of a trade union.
e. Physical or mental health or condition.
f. Sexual life.

Data Protection Principle

Currently there are eight Data Protection Principles; this will be reduced to six with individual's rights and the transfer of data overseas being addressed in their own sections of the Regulations. The Data Controller is responsible for compliance with the principles, e.g. by documenting the decisions taken about a processing activity.

All personal data must be:

a. Processed lawfully, fairly and in a transparent manner.
b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
c. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
d. Accurate and kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay.
e. Kept in a form which permits identification of data subjects for no longer than is necessary.
f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Principle 1

All personal data must be processed lawfully. In practice, this means you must:

- Have legitimate grounds for collecting and using the personal data.
- Not use the data in ways that have an adverse effect on the individuals concerned.
- Be clear 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.
- Make sure you do not do anything unlawful with the data.

On the 25th May 2018, the current Data Protection Act (DPA) was replaced by the EU General Data Protection Regulations (GDPR).

Principle 2
All personal data must be collected for specified and legitimate purposes and not processed further. In practice, this means 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 legislation's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data.
- Comply with what the legislation says about notifying the Information Commissioner.
- Ensure that if you wish to use personal data for any additional purpose or different purpose, the new use or disclosure is fair.

Principle 3
All personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. In practice, this means you should ensure that:

- You hold personal data about an individual that is sufficient for the purpose.
- You do not hold more information than you need for that purpose.

Principle 4
All personal data must be accurate and kept up to date. Personal data that is inaccurate should be erased or rectified. In practice, it means that you will need to:

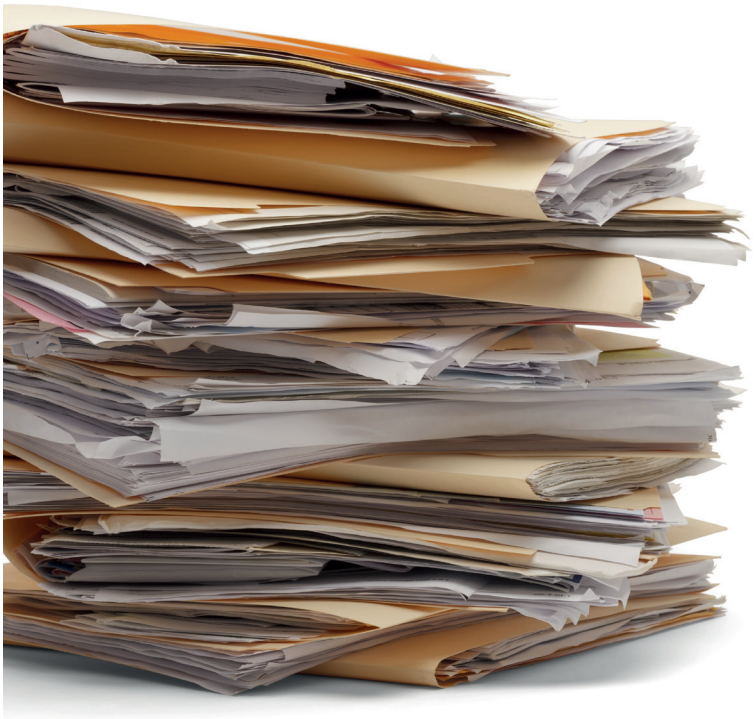
- Take reasonable steps to ensure the accuracy of any personal data you obtain.
- Ensure that the source of any personal data is clear.
- Consider any challenges to the accuracy of information.
- Consider whether it is necessary to update the information.

Principle 5
All personal data must be kept for no longer than is necessary. In practice, it means that you will need to:

- Review the length of time you keep personal data.
- Consider why you hold information and whether you need to retain it.
- Securely delete information that is no longer needed.
- Update, archive or securely delete information if it goes out of date.

Principle 6
All personal data must be processed in a secure manner using appropriate technical or organisational measures. 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.
- Respond to any breach of security swiftly and effectively.

Lawful Processing

To comply with GDPR, the processing of data must be supported by a specific legal requirement; there are six grounds for processing personal data and ten grounds for processing special categories of data that can be selected from and the selected option must be documented, for example in the form of a Privacy Notice.

Obtaining Consent

Consent needs to be given by clear positive action and evidence of this will need to be kept.

Children's Personal Data

There is an enhanced requirement, when collecting children's personal data, to ensure that privacy notices are written in a clear and plain way that the child would understand, and in some cases the consent of a parent / guardian will be required.

Individual Rights

Previously known as principle 6, Individuals Rights now form their own section of the legislation.

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights related to automated decision making and profiling.

Right to be informed

The right to be informed means organisations need to be clear about how they are going to use data. This can be done using a privacy notice.

Right of access

Individuals have the right to obtain:

- Confirmation that their data is being processed.
- Access to their personal data.

Supplementary information e.g. information that should be provided in a privacy notice.

- Subject Access Requests - under GDPR organisations:
- Will no longer be able to charge a fee.
- Have one month to respond (rather than 40 days).
- Can refuse to respond (or charge a reasonable fee) if the request is 'manifestly unfounded or excessive'.
- Can ask the Subject to specify their request if a lot of data is processed about them.

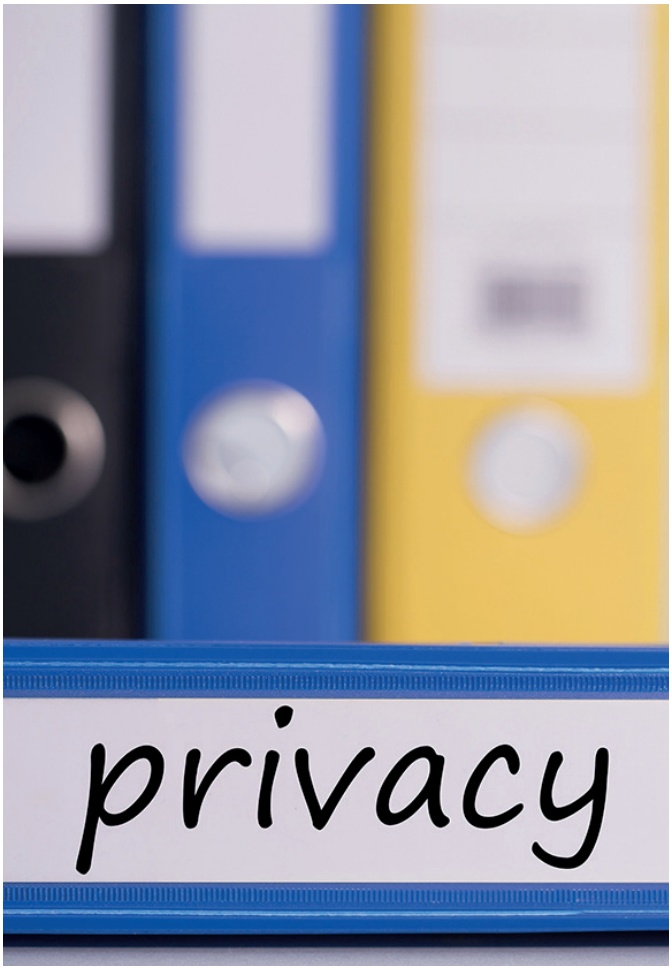
If the request is made electronically, the response should be provided electronically (best practice is to permit remote access to a secure self-service system allowing the individual to gain direct access to their information).

Right to rectification

Individuals are entitled to have their personal data rectified if it is inaccurate or incomplete. Organisations will be required to acknowledge such requests within one month, and complete the request within two months OR explain to the individual why action will not be taken.

Right to erasure or 'right to be forgotten'

This enables an individual to request the deletion or removal of personal data. There are many reasons why an individual has the right to have their personal data erased and an equal number of reasons why a request can be refused.



Right to restrict processing

Individuals have a right to 'block' the processing of their personal data (but not erasing it). When processing is restricted, organisations are permitted to store the personal data, but not to further process it. They can retain just enough information about the individual to ensure that the restriction is respected.

Right to data portability

This allows individuals to obtain and reuse their personal data for their own purposes across different services; to have their data moved, copied or transferred easily from one IT environment to another in a safe and secure way, e.g. when switching banks, utility providers. Organisations will be required to acknowledge such requests within one month, and complete the request within three months.

Right to object

Individuals have the right to object to:

- Processing based on 'legitimate interests' or 'the performance of a task in the public interest / exercise of official authority' (including profiling).
- Direct marketing (including profiling).
- Processing for the purposes of scientific / historical research and statistics.

Rights related to automated decision making and profiling

This is the right to have a human intervene in decision making if the automated decision results in a negative decision being made.

If an organisation shares an individuals' data with their supply chain they must ensure that these rights are complied with by all third parties. They must also inform the individual about the third parties to whom the data has been disclosed.

Transfer of Data

The transfer of data outside of the European Union will be permitted, in much the same way as by the DPA, but the process must comply with certain conditions of transfer. It also states appropriate safeguards that should be applied when transferring data.

Accountability

All organisations will be required to demonstrate that they comply with the Regulations by introducing process documents detailing how they will comply, not just by maintaining records of compliance.

Organisations are required to put into place governance measures. These measures should minimise the risk of breaches and uphold the protection of personal data.

Data Protection Impact Assessments and Privacy by Design

Data Protection Impact Assessments are the same as the current Privacy Impact Assessments but the GDPR states when these are needed and what they should contain.

Privacy by Design should also be worked into all new products, solutions, service offerings etc.

Data Protection Officer (DPO)

Not all Organisations will need to appoint a Data Protection Officer (DPO). DPO should have professional experience and knowledge of data protection law. The name and contact details of the DPO should be widely available to all who may need to use them, and shared with the ICO.

Breach Notification

A breach is defined as something that will result in 'a risk to the rights and freedoms of individuals'. All organisations have a duty to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected. Breaches will need to be reported to the ICO within 72 hours and must contain certain pieces of information. Failure to report a breach may result in a fine of up to £8.8m or 2% of global turnover.

Fines

The GDPR increases this to £17m or 4% of global turnover, whichever is greater, for a serious breach.

The Medical Reports Act 1998

M

This Act allows access to medical reports prepared for employment or insurance purposes by a medical practitioner, but only with the permission of the person who is the subject of the report, and that person must be informed of his/her rights under the Act by whoever requires the report.

If requested, the subject of the report can see it before the person who requires it, and request that the medical practitioner make amendments to the report before giving it to the employer or insurer. If the medical practitioner refuses to make the amendments, then the subject of the report can ask that a statement of his/her views be attached to it before it is passed on.

This Act allows access to medical reports prepared for employment or insurance purposes by a medical practitioner.