



# Data protection factsheet

## What is the GDPR?

The General Data Protection Regulation forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). This replaces the Data Protection Act 1988. The main provisions of this applied from 25 May 2018, which means all business should already be applying the principles of the GDPR in their daily work activities.

## Who does it apply to?

The GDPR applies to businesses who may be called a 'controller' or 'processor'. A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller. As a landscape contractor or designer, it is most likely that you are a controller, since you will frequently be deciding what personal data to collect (for example, the names, email addresses, telephone numbers and addresses of clients) and how this information will be recorded e.g. on a phone, in a book or via email. Note that GDPR applies to historic, current and all future electronic and manual records held by your company.

## What is personal data?

Personal data only includes information relating to natural persons who can be identified or who are identifiable, directly from the information in question (e.g. name, address, email, NI number); or who can be indirectly identified from that information in combination with other information (e.g. Computer's IP address). As a landscape contractor or garden designer, it is likely you will record personal data from clients which includes their name, address and email address.

Information about companies or public authorities is not personal data, however, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable, and the information relates to them as an individual, may constitute personal data.

## What are my responsibilities?

Whilst the owners, directors or management team are directly accountable, all employees within a business have a responsibility to ensure their business conforms with the General Data Protection Regulation.

Before collecting personal information, you must identify valid grounds under the GDPR (known as a 'lawful basis') for collecting and using personal data from your customers and prospective customers. There are six of these lawful bases, which are listed below:

1. Consent
2. Contract
3. Legal obligation
4. Vital interests
5. Public task
6. Legitimate interests

For example, you may record information such as a name and address to provide a quote or a service, offer credit terms and get paid. These examples fall under the lawful basis of processing by way of "contract" as without this basic information you could not provide your services.

You must ensure that you do not do anything with the data in breach of any other laws, such as give it to others without permission (see consent) or store it in an unsecure way. Note that storing data in an unsecure way could include writing client names, addresses and phone numbers in a book which is not thoughtfully looked after, or on computer or phone which is not password protected. You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned – for example, share or sell it. You must be clear, open and honest with people from the start about how you will use their personal data.

## What are the rights of my customers and potential customers?

The individuals whose information you collect and use have particular rights. There are eight of these, which are:

1. The right to be informed (i.e. what exactly will you do with their information?)
2. The right of access (i.e. you must be able to give individuals a copy of their personal data that you hold on them)
3. The right to rectification (i.e. individuals are entitled to have their personal information corrected)
4. The right to erasure (also known as the right to be forgotten, in some circumstances an individual can request a business deletes information held about them)
5. The right to restrict processing (in some circumstances an individual can limit the way in which a business uses their data)
6. The right to data portability (this right gives individuals the right to receive information they originally provided to a business in a format that is organised and commonly used)
7. The right to object (in some circumstances, an individual can object to businesses processing their data in a specific way)
8. Rights in relation to automated decision making and profiling. (in some circumstances, businesses can be prevented from using automated – computer controlled – decisions)

More detail on these is included in the “Further reading” section, below.

## What is consent?

As discussed in the responsibilities section, as a business you should ensure you process (collect, record, organise, store or use) data on a lawful basis. As a landscape contractor or garden designer, in most cases you will be processing data under the lawful basis of ‘contract’. If, for example, you wish to contact a customer regarding additional services your business can offer, or sign a customer to direct marketing materials, a different lawful basis is required – ‘consent’ is one such example of a different lawful basis.

The definition of consent in GDPR is similar to the definition of consent outside of GDPR! Under GDPR, consent is given by an individual to a business when s/he gives a specific and informed decision of his or her wishes either via a statement or clear affirmative action (e.g. ticking a box) called an opt-in. For example, consent may be gained from an individual to send them additional information on relevant products by using the following text as part of a contract for works:

*I consent to [your company name] sending me additional information on relevant and complementary products or services, from time to time, by the following methods:*

email  letter  telephone  text message

The wording above is found in a consent form which is designed to be used in conjunction with the BALI domestic contract. Both of these documents are free for BALI members to use and can be found on the BALI website.

You must keep clear records to demonstrate consent you hold.

The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw and offer them easy ways to withdraw consent at any time. (You may wish to use the consent form provided by BALI)

### What is a breach and what do I do?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. For example, losing a book in which you keep client addresses is classed as a data breach, as is losing a mobile telephone which contains the names and address of clients.

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority (currently this is the ICO). You must do this within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals. This is based on material harm to individuals, scale of impact, likelihood of recurrence, risk to others and so forth.

You must also keep a record of any personal data breaches, regardless of whether you are required to notify the authority.

### Where can I find further information

For further information you can visit the ICO Website at <https://ico.org.uk/> or call the Small Business Helpline on **0303 123 1113**.

## Further reading

### The rights of individuals

Below are some further details and explanations concerning the rights of individuals:

1. **The right to be informed** – to be told their data is being collected and used.
2. **The right of access** – to be given a copy of the information you hold on them.
3. **The right to rectification** – to be able to correct any information you hold on them that is incorrect.
4. **The right to erasure** – to be able to have their information taken off your systems, both electronically and in hard copy (certain exclusions apply – please refer to the ICO website at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/>).
5. **The right to restrict processing** – individuals have the right to request you restrict the processing of their personal data if the individual contests the accuracy of their personal data and you are verifying the accuracy of the data; the data has been unlawfully processed; you no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or the individual has objected to you processing their data and you are considering whether your legitimate grounds override those of the individual.
6. **The right to data portability** – this gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It does not apply to paper copies.
7. **The right to object** – individuals have the right to object to the processing of their personal data. This effectively allows individuals to ask you to stop processing their personal data. The right to object only applies in certain circumstances. Whether it applies depends on your purposes for processing and your lawful basis for processing. An individual can ask you to stop processing their personal data for direct marketing at any time. This is an absolute right and there are no exemptions or grounds for you to refuse. Therefore, when you receive an objection to processing for direct marketing, you must stop processing the individual's data for this purpose.
8. **Rights in relation to automated decision making and profiling** – the GDPR has provisions on automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process. Further information, if applicable to you, can be found on the ICO website at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/>.