# GDPR PRIVACY POLICY FOR WEBSITE

**Disclaimer: this sample policy is provided for general information purposes only and does not constitute legal advice. In order to be fully effective, it should be customised to suit the individual procedures of your organisation.**

This privacy policy tells you what will happen to any personal data that you provide to (*name of organisation*) as a result of using this website or contacting this organisation. We fully understand that your privacy is important to you and that you care about how your personal data is used and shared online and we will take account of, and respect, your concerns.

This policy explains how we will use, and protect, the information that we gather, whether it be through this website, by way of telephone or personal conversations or through our normal business contacts with you. Please read this privacy policy carefully and ensure that you understand it. Details are given below of contacts should you wish to ask questions but please note that acceptance of this privacy policy and our cookie policy (see "Cookies" below) is required to make full use of our site.

**Our details**

| | |
|---|---|
| Organisation's name | SM FACILITIES MANAGEMENT LTD |
| Address | SQUARED, BRAMINGHAM BUSINESS CENTRE LU3 4BU |
| Telephone number | 01582593819 |
| Email address (eg GDPR@ …) | info@smfacilities.co.uk |

We are registered with the Information Commissioner's Office (ICO).

Our Data Protection Officer (DPO) (*add name*) can be contacted at (*add email*).

(*Alternatively, if the organisation does not have a DPO, give the name and contact details of a representative who can deal with enquiries regarding data protection.*)

**Your rights**

Under the General Data Protection Regulation (GDPR), you have the right to be informed about:

- the collection and use of your personal data
- our purposes for processing that data
- the retention periods for storing your data (or a guarantee that it will be kept only for as long as necessary)
- who it will be shared with (both in this country and, if applicable, in others: in this case, we will inform you of the safeguards which are applied in that country)
- the legal basis under which we process your data
- the right to withdraw your consent (if consent is the legal basis for processing)
- our "legitimate interest" in processing your data (if that interest is the legal basis for processing)
- details of any data we collect about you from a third party (such as publicly-available information)
- the right to lodge a complaint with the ICO
- details of the existence of automated decision-making, including profiling (if applicable).

You also have the right to information that is concise, transparent, intelligible, easily accessible and presented to you in clear and plain language rather than in "legalese". We would encourage you to get in touch with the contact given above if you have any questions about this policy statement or our procedures with regard to data processing. This will not in any way affect your right (mentioned above) to complain to the ICO.

Finally, we commit to informing you if, at any time, we update our privacy information and always to seek permission if we plan to use your personal data for a new purpose.

**The information we collect**

We process and store details of your*:

- name
- chosen mode of address (Mrs, Ms, etc)
- job title
- date of birth
- address
- IP address
- email address
- username(s)

*(*delete if necessary).*

These details will typically be provided when you take out a subscription or sign up to receive a newsletter or future details of our products/services. We only keep them for as long as necessary and you may, at any time, contact us to ask for them to be removed (see "the right to be forgotten" below).

*(Where the organisation collects sensitive personal information — such as biometric data or details of racial or ethnic origin, religious or philosophical beliefs or trade union membership — or financial information, it should make clear the extra levels of security — such as encryption — that will be applied to its protection.)*

**Why do we need this information?**

We use the information that we collect and store about you to:

- provide our products/services
- manage invoices and accounts
- deliver marketing and events information
- invite participation in polls and surveys.

*(Note: this is not an exhaustive list and should be amended or added to, to reflect the organisation's business model.)*

**The legal basis under which we collect and store data**

There are six possible legal grounds under the GDPR. These are:

1. consent
2. fulfilment of a contact
3. legitimate interests
4. vital interests
5. public task
6. legal obligation.

*Each organisation must decide which of these applies to the data they process and explain how and why that is the case. For example, "consent" to use personal data must be freely given and be provided in an intelligible and easily accessible form, using clear and plain language (not pre-ticked boxes or any other method of default consent). It must be as easy to withdraw consent as it is to give it.*

*"Legal obligations" is a lawful basis if an organisation needs to process the personal data to comply with a common law or statutory obligation. The ICO makes clear that "you cannot rely on this lawful basis if you have discretion over whether to process the personal data, or if there is another reasonable way to comply".*

*"Vital interests" is unlikely to feature in most organisation' routine plans as it covers the need to process the personal data to protect someone's life. If the person's vital interests can reasonably be protected in another less intrusive way, this basis will not apply.*

*"Public task" is mainly relevant to public authorities or to organisations that exercise official authority or carry out tasks in the public interest. Again, to quote the ICO: "If you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply."*

*This leaves "legitimate interests" as the legal basis most likely to be used, if consent does not apply. It is the most flexible, and likely to be most appropriate where you are using people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.*

*If you decide that "legitimate interests" is the legal basis on which you are collecting and processing personal data, it would be advisable to include in your data protection policy a statement to the effect that:*

**Legal basis — legitimate interests**

"This organisation has carried out a legitimate interests assessment (LIA) which can be seen on request. In doing so, we have checked that the processing is necessary and that there is no less intrusive way to achieve the same result. We will only use your data in ways that you would reasonably expect, unless we have a very good reason. We will not use your data in ways that you would find intrusive or which could cause you harm and we have considered and introduced safeguards to reduce the impact where possible.

If we process children's data, we take extra care to make sure we protect their interests. In using this basis for processing data, we will make sure that your interests, as protected by the GDPR, are not undermined by our legitimate interests."

**Applying the data protection principles**

This organisation is committed to applying the principles set out in the GDPR. To that end, we will always strive to ensure that:

- personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- our procedures are adequate, relevant and limited to what is necessary in relation to the purposes for which they are put in place
- the data we collect are accurate and, where necessary, kept up to date, every reasonable step will be taken to ensure that data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- data are kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed
- data are processed in a manner that ensures their appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

**Better by design**

In applying the above principles, this organisation recognises that it has a general obligation to implement technical and organisational measures to show that it has considered and integrated data protection into all data processing activities. We have built safeguards into products and services from the earliest stage of development and privacy-friendly default settings are the norm for all our services. All of our employees are trained in the requirements of GDPR and as far as possible we aim to ensure that contracts, website designs, publicity materials and HR policies are all in line with the GDPR requirements.

**Access to your data**

On receipt of a request for access to the data which we hold about you, we will respond without delay and at the latest within one month of receipt. Information will be provided free of charge although a reasonable fee may be applied when a request requires excessive work, particularly if it is repetitive. This fee will reflect the amount of administrative work involved.

**The right to be forgotten**

Also known as data erasure, the "right to be forgotten" set out in the GDPR entitles you to ask any data controllers (including this organisation) to erase your personal data and to cease further dissemination. You can make such a request either verbally or in writing and we will respond as quickly as possible, and at the latest within one month. We understand that there is a particular emphasis on the right to erasure if the request relates to data collected from children and such requests will always be given the highest priority.

Please note, however, that there are certain circumstances in which the right to erasure may not apply. These include where processing is necessary for one of the following reasons:

- to comply with a legal obligation

- to exercise the right of freedom of expression and information
- for the performance of a task carried out in the public interest or in the exercise of official authority
- for the establishment, exercise or defence of legal claims.

In addition, any organisation is allowed to refuse to comply with a request for erasure if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. We will, however, explain and justify any such refusal.

**Right to be informed**

Within one month of collecting your personal data, we will inform you of the purposes for processing that data, the retention periods and with whom it will be shared. Any information which is provided to you will be concise, transparent, intelligible, easily accessible and presented in clear and plain language.

**Right to rectification**

Either verbally or in writing, you may ask for inaccurate personal data to be rectified, or to be completed if it is partial. We will respond as quickly as possible and certainly within the one month time period allowed under the GDPR. In the unlikely event that there is disagreement over the accuracy of the data, we will do our best to resolve this and you will, of course, have right to take the matter to the ICO if we cannot reach agreement. If that situation arises, we are prepared to consider restricting processing of the contested data during the time it takes to resolve the issue with the ICO.

**Children**

Under the GDPR, only children aged 13 or over are able provide their own consent. For those under this age, we will seek consent from whoever holds parental responsibility or, if we are using a different legal basis, will inform that person accordingly. We are fully aware that children have the same rights as adults over their personal data and are committed to ensuring full protection for them at all times.

**Right to data portability**

This organisation recognises that, under the GDPR, you must be able to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The requested information will be provided free of charge in a structured, commonly used and machine-readable form. However, it should be noted that the right to data portability only applies:

- to personal data an individual has provided to a controller
- where the processing is based on the individual's consent or for the performance of a contract
- when processing is carried out by automated means.

**Right to object**

You 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 purposes of scientific/historical research and statistics.

We will stop processing personal data for direct marketing purposes as soon as an objection is received.

**Automated decision-making and profiling**

Profiling refers to the automated processing of personal data to evaluate certain things about an individual. Together with making a decision solely by automated means, it is covered by the GDPR and will require the individual's explicit consent. We will only collect the minimum amount of data needed and will retain it only for as long as is necessary. Anyone affected by an automatic decision has the right to ask for it to be reconsidered and we have additional checks in place for profiling/automated decision-making systems to protect vulnerable groups such as children.

**Data breaches**

While we will take all appropriate measures to prevent illegal access to your data, we have to prepare for that possibility. Should there be a significant data breach affecting your data and rights, we will notify you (and the ICO) as soon as possible. To minimise any possible danger, we will use encryption and/or pseudonymisation where it is appropriate to do so. We will also have backup systems in place in the event that an outside organisation attempts to disrupt access to our data,

**International transfers**

*(If an organisation sends data to countries outside the EU.)*

Given that all members of the European Economic Area (EEA) (that is, all EU Member States, plus Norway, Iceland, and Liechtenstein) have to comply with the Union's standards on data protection, and particularly with the GDPR, then we can legally transfer data to those countries. However, if we have reason to send data to non-EEA countries, we recognise that they must have equivalent standards in place. This is not a matter for individual organisations to assess but must be based on, for example, standard data protection clauses in the form of template transfer clauses adopted by the European Commission or compliance with an approved Code of Conduct approved by the ICO.

Should such transfers take place, we will make it clear which of these provisions we have adopted to ensure safety. (Among the countries recognised by the commission as having equivalent standards are Switzerland, New Zealand and Canada. USA companies that have certified with the EU-US *Privacy Shield* programme are also considered to be safe destinations).

**Cookies**

A cookie is a small text file placed on your computer or device by our site when you visit certain parts of it and/or use certain of its features. For example, we may monitor how many times you visit, which pages you go to, traffic data, location data, weblogs and other communication data whether required for billing purposes or otherwise. We may also look at the originating domain name of a user's internet service provider, IP address, operating system and browser type. This information helps us to build a profile of our users. Where appropriate, this data will be aggregated or statistical, which means that we will not be able to identify you individually.

Cookies are also used to remember your settings (language preference, for example) and for authentication (so that you do not have to repeatedly sign in). You can set your browser not to accept cookies and there are a number of websites which explain how to remove cookies from your browser. However, it is possible that some of our website features may not function as a result.

**Third party websites**

Please note that there are some links on our website to other sites where you may find useful information. This does not indicate a general endorsement of those sites and, as we have no control over how data is collected, stored, or used by other websites, we would advise you to check their privacy policies before providing any data to them.