Data Protection Policy

Introduction

We comply with the GDPR and any data held by us is held on the following basis provided in the GDP: Consent, Contract, Legal Obligation, Vital interests, Public task or legitimate interest and is only such data typically name, Email, phone number and address- necessary for us to contact you and payment details if we pay money to you. If you have any issues or would like to read our data protection policy or object to us holding your data and would like us to delete it please email mailto:info@willmottgrant.co.uk?subject=Data Protection Policy

The organisation is committed to being transparent about how it collects and uses the personal data including, in particular, the data of our employees, sub-contractors, people we engage on a freelance basis and actual and potential clients/customers of our services. This policy applies to the personal data of all such persons.

Data Protection Principles

The organisation processes personal data in accordance with the following data protection principles:

• The organisation processes personal data lawfully, fairly and in a transparent manner.

• The organisation collects personal data only for specified, explicit and legitimate purposes.

• The organisation processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.

• The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.

• The organisation keeps personal data only for the period necessary for processing.

• The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The organisation tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. Where the organisation relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

The Legal Basis on Which We Hold Personal Data

We hold personal data under the following permitted reasons provided by the GDPR- so one of these reasons will apply to your data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell him/her:

• whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
• to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
• for how long his/her personal data is stored (or how that period is decided);
• his/her rights to rectification or erasure of data, or to restrict or object to processing;
• his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and
• whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

The organisation will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

To make a subject access request, the individual should send the request to mailto:info@willmottgrant.co.uk?subject=Data Protection Policy.
In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify his/her identity and the documents it requires.

The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the organisation processes large amounts of the individual's data, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify him/her that this is the case and whether or not it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

• rectify inaccurate data;
• stop processing or erase data that is no longer necessary for the purposes of processing;
• stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
• stop processing or erase data if processing is unlawful; and
• stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

To ask the organisation to take any of these steps, the individual should send the request to mailto:info@willmottgrant.co.uk?subject=Data Protection Policy

Data security

The organisation takes the security of personal data seriously. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Data breaches

If the organisation discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect.