

<p>EPC Choice Ltd Data Protection Policy 22<sup>nd</sup> May 2018</p>
---

## **1. Introduction**

This Policy sets out the obligations of EPC Choice Ltd (“the Company”) with regard to data protection and the rights of website users, customers, clients, surveyors, portal users and business contacts (“data subjects”) in respect of their personal data under the Data Protection Act 1998 (“the Act”). Under the Act, “personal data” is defined as data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller (the Company in this context), 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.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law but also to the spirit of the law and places a high premium on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

The Company is registered with the Information Commissioner as a data controller under the register held by the Information Commissioner pursuant to Section 19 of the Act.

## **2. The Data Protection Principles**

This Policy aims to ensure compliance with the Act. The Act sets out eight principles with which any party handling personal data must comply. All personal data:

- 2.1 Must be processed fairly and lawfully, meaning that at least one of the following conditions must be met:
  - 2.1.1 The data subject has given his or her consent to the processing;
  - 2.1.2 The processing is necessary for the performance of a contract to which the data subject is a party, or for the taking of steps at the request of the data subject with a view to entering into a contract;
  - 2.1.3 The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract;
  - 2.1.4 The processing is necessary in order to protect the vital interests of the data subject;
  - 2.1.5 The processing is necessary for the administration of justice, for the exercise of any functions of either House of Parliament, for the

exercise of any functions conferred on any person by or under any enactment, for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or for the exercise of any other functions of a public nature exercised in the public interest by any person;

2.1.6 The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data is disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

2.2 Where the personal data is sensitive personal data (defined below in Part 4 of this Policy), at least one of the following conditions must be met:

2.1.7 The data subject has given his or her explicit consent to the processing of the personal data;

2.1.8 The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment;

2.1.9 The processing is necessary in order to protect the vital interests of the data subject or another person in a case where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject, or in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;

2.1.10 The processing is carried out in the course of the legitimate activities of any body or association which is not established or conducted for profit, and exists for political, philosophical, religious or trade-union purposes, is carried out with appropriate safeguards for the rights and freedoms of data subjects, relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and does not involve disclosure of the personal data to a third party without the consent of the data subject;

2.1.11 The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject;

2.1.12 The processing is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), the processing is necessary for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights;

2.1.13 The processing is necessary for the administration of justice, for the

exercise of any functions of either House of Parliament, for the exercise of any functions conferred on any person by or under an enactment, or for the exercise of any functions of the Crown, a minister of the Crown or a government department;

2.1.14 The processing is either the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation, or any other processing by that person or another person of sensitive personal data so disclosed, and is necessary for the purposes of preventing fraud or a particular kind of fraud;

2.1.15 The processing is necessary for medical purposes and is undertaken by a health professional, or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional;

2.1.16 The processing is of sensitive personal data consisting of information as to racial or ethnic origin, the processing is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and is carried out with appropriate safeguards for the rights and freedoms of data subjects.]

- 2.3 Must be obtained only for specified and lawful purposes and shall not be processed in any manner which is incompatible with those purposes;
- 2.4 Must be adequate, relevant and not excessive with respect to the purposes for which it is processed;
- 2.5 Must be accurate and, where appropriate, kept up to date;
- 2.6 Must be kept for no longer than is necessary in light of the purpose(s) for which it is processed;
- 2.7 Must be processed in accordance with the rights of data subjects under the Act (for which, see Part 3 of this Policy);
- 2.8 Must be protected against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures; and
- 2.9 Must not be transferred to a country or territory outside of 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.

### **3. Rights of Data Subjects**

Under the Act, data subjects have the following rights:

- The right to access a copy of their personal data held by the Company by means of a Subject Access Request (for which, see Part 8 of this Policy);
- The right to object to any processing of his or her personal data that is likely to cause (or that is causing) damage or distress. Data subjects should make any such objection in writing to Christopher Grant Data Protection Office EPC Choice Ltd and the Company shall respond within 21 days either notifying the data subject of its compliance, or explaining why the Company feels that any aspect of the data subject's request is unjustified;
- The right to prevent processing for direct marketing purposes;
- The right to object to decisions being taken by automated means (where such decisions will have a significant effect on the data subject) and to be informed when any such decision is taken (in which case the data subject has the right to require the data controller (by written notice) to reconsider the decision);
- The right to have inaccurate personal data rectified, blocked, erased or destroyed in certain circumstances;
- The right to claim compensation for damage caused by the Company's breach of the Act.

### **4. Personal Data**

Personal data is defined by the Act as data which relates to a living individual who can be identified from that data or from that 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.

The Act also defines "sensitive personal data" as personal data relating to the racial or ethnic origin of the data subject; their political opinions; their religious (or similar) beliefs; trade union membership; their physical or mental health condition; their sexual life; the commission or alleged commission by them of any offence; or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

The Company only holds personal data that is directly relevant to its dealings with a given data subject. That data will be collected, held, and processed in accordance with the data protection principles and with this Policy. The following data may be collected, held and processed by the Company:

- Name, because we need to know who you are;
- Telephone Numbers, In case we need to call you;
- Your Home or Business address, in case we need to write to you;
- Your email address, because we will from time to time send you information;

## **5. Processing Personal Data**

Any and all personal data collected by the Company (as detailed in Part 4 of this Policy) is collected in order to ensure that the Company can provide the best possible service to its customers, and can work effectively with its partners, associates and affiliates and efficiently manage its employees, contractors, agents and consultants. The Company may also use personal data in meeting certain obligations imposed by law.

Certain data collected by the Company, such as IP addresses, certain information gathered by cookies, pseudonyms and other non-identifying information will nonetheless be collected, held and processed to the same standards as personal data.

Personal data may be disclosed within the Company, provided such disclosure complies with this Policy. Personal data may be passed from one department to another in accordance with the data protection principles and this Policy. Under no circumstances will personal data be passed to any department or any individual within the Company that does not reasonably require access to that personal data with respect to the purpose(s) for which it was collected and is being processed.

In particular, the Company shall ensure that:

- All personal data collected and processed for and on behalf of the Company by any party is collected and processed fairly and lawfully;
- Data subjects are always made fully aware of the reasons for the collection of personal data and are given details of the purpose(s) for which the data will be used;
- Personal data is only collected to the extent that is necessary to fulfil the purpose(s) for which it is required;
- All personal data is accurate at the time of collection and kept accurate and up to date while it is being held and/or processed;
- No personal data is held for any longer than necessary in light of the purpose(s) for which it is required;
- A suitable online privacy policy is implemented, maintained and followed;
- Whenever cookies or similar technologies are used online by the Company, they shall be used strictly in accordance with the requirements of the Privacy and Electronic Communications Regulations, providing full details of cookie use and guidance on privacy;
- Individuals are provided with a simple, accessible method of amending any data submitted by them online;
- Individuals are informed if any data submitted by them online cannot be fully deleted at their request under normal circumstances (for example, because a file uploaded by a user has been backed up) and how to request that the Company deletes any other copies of that data, where it is within the individual's right to do so;
- All personal data is held in a safe and secure manner, as detailed in Part 6 of this Policy, taking all appropriate technical and organisational measures to protect the data;

- All personal data is transferred securely, whether it is transmitted electronically or in hard copy, using a full encrypted server and secure on-site storage facility.
- No personal data is transferred outside of the European Economic Area (as appropriate) without first ensuring that the destination country offers adequate levels of protection for personal data and the rights of data subjects; and
- All data subjects can fully exercise their rights with ease and without hindrance.

## **6. Data Protection Procedures**

The Company shall ensure that all of its employees, agents, contractors, or other parties working on behalf of the Company comply with the following when working with personal data:

- All emails containing personal data must be encrypted using Advanced Encryption Standard;
- Personal data may be transmitted over secure networks only – transmission over unsecured networks is not permitted in any circumstances;
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Recorded Delivery;
- No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from The Data Protection Officer.
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;
- No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of Data Protection Officer;
- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

- Any unwanted copies of personal data (i.e. printouts or electronic duplicates) that are no longer needed should be disposed of securely. Hardcopies should be shredded and electronic copies should be deleted securely using our in-house data destruction software;
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of The Data Protection Officer and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.
- No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Act (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);
- All personal data stored electronically should be backed up daily with backups stored onsite in a secure location. All backups should be encrypted using Advance Encryption Standard;
- All electronic copies of personal data should be stored securely using passwords and Advance Encryption Standard data encryption;
- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by the Company is designed to require such passwords;
- Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
- All personal data held by the Company shall be regularly reviewed for accuracy and completeness. Where the Company has regular contact with data subjects, any personal data held about those data subjects should be confirmed at least every three months. If any personal data is found to be out of date or otherwise inaccurate, it should be updated and/or corrected immediately where possible. If any personal data is no longer required by the Company, it should be securely deleted and disposed of using File Shredder Software;
- Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of Christopher Grant EPC Choice Data Protection Officer to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service. Such details should be checked at least every 3 months.

## 7. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

- The Company has appointed Christopher Grant EPC Choice Data Protection Officer as its Data Protection Officer with the specific responsibility of overseeing data protection and ensuring compliance with this Policy and with the Act. The Data Protection Officer shall in particular be responsible for:
  - Overseeing the implementation of, and compliance with this Policy, working in conjunction with the relevant employees, managers and/or department heads, agents, contractors and other parties working on behalf of the Company;
  - Organising suitable and regular data protection training and awareness programmes within the Company;
  - Reviewing this Policy and all related procedures not less than every 3 months;
- All employees, agents, contractors, or other parties working on behalf of the Company are made fully aware of both their individual responsibilities and the Company's responsibilities under the Act and under this Policy, and shall be provided with a copy of this Policy;
- Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to and use of personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;
- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;
- The Performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Act and this Policy by contract;
- All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Act;
- Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages,



loss, claims or proceedings which may arise out of that failure.

## **8. Access by Data Subjects**

A data subject may make a subject access request (“SAR”) at any time to find out more about the information which the Company holds about them.

- SARs should be made in writing, addressed to Christopher Grant EPC Choice Data Protection Officer.
- A SAR may be made using the Company’s Subject Access Request Form, but does not have to be, and if it is not, it should be clearly identifiable as a SAR.
- SARs must make it clear whether it is the data subject themselves that is making the request or whether it is a person acting on his or her behalf. In either case, proof of identity must be provided. If the SAR is made on another’s behalf, the individual making the request must provide clear evidence of their authorised capacity to act on behalf of the data subject.
- The Company currently requires a fee of £10 (the legal maximum) for each SAR, payable by cheque. A fee of £2 shall be required for access to a credit file.

Upon receipt of a SAR the Company shall have a maximum period of 40 calendar days within which to respond fully, but shall always aim to acknowledge receipt of SARs within 5 working days. The following information will be provided to the data subject:

- Whether or not the Company holds any personal data on the data subject;
- A description of any personal data held on the data subject;
- Details of what that personal data is used for;
- Details of how to access that personal data and how to keep it up to date;
- Details of any third-party organisations that personal data is passed to; and
- Details of any technical terminology or codes.

## **9. Notification to the Information Commissioner’s Office**

As a data controller, the Company is required to notify the Information Commissioner’s Office that it is processing personal data. The Company is registered in the register of data controllers, registration number: ZA002276.

Data controllers must renew their notification with the Information Commissioner’s Office on an annual basis. Failure to notify constitutes a criminal offence.

Any changes to the register must be notified to the Information Commissioner’s Office within 28 days of taking place.

The Data Protection Officer shall be responsible for notifying and updating the Information Commissioner’s Office.

**10. Implementation of Policy**

This Policy shall be deemed effective as of 22/05/2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved & authorised by:

**Name:** Christopher Grant

**Position:** Director

**Date:** 21/05/2018

**Due for Review by:** 21/06/2019

**Signature:** 