CRBDirect

# DATA PROTECTION POLICY AND PROCEDURE

Our activity involves the collection of personal data and may involve the collection of sensitive personal data.

Data for the purposes of our products and services includes:

- Customer personal information;
- Customer transactional data; and
- Special categories of data.

We only store and processes data in accordance with the data protection principles contained in the Data Protection Act 1998, and also, in line with the General Data Protection Regulation which is coming into force on 25th May 2018.

We have not identified any aspect of our products and services which breaches, or is likely to breach, the requirements of the Data Protection Act 1998.

We will retain successful applicants' information by way of archiving and encryption within our bespoke CRM system. We will delete personal data which is not necessary to hold (such as additional supporting documents) once an application has been completed. We will hold transaction and contact information for the purposes of complaints and this will be securely deleted after a period of three years.

Data is retained in connection with our products and services for a period of three months in the case of data subjects who have engaged with us but have not become customers. If we are unable for any reason to provide an exact timescale for data retention of particular information, we will provide a framework of the criteria used to determine this period.

CRBDirect

The Information Commissioner enforces the Data Protection Act 1998, and the General Data Protection Regulation; which give individuals the right to know what information is held about them and provides the framework to ensure that personal information is handled correctly.

Our legal responsibilities under the Act are:

• To notify the Information Commissioner we are processing information;

• To process the personal information in accordance with the eight principles of the Act; and

• To answer subject access requests received from individuals;

Brett Adams is responsible for overseeing Data Protection. Their responsibilities include:

• Ensuring that the Information Commissioner is notified and that the notification is kept up to date. Renewal of the Firm's registration costs an annual fee, no VAT charge and is payable to the Information Commissioner's Office;

• Ensuring that the people whose information we hold, know that we have it, and that they are likely to understand what it will be used for;

• Ensuring that there are sufficient safety measures in place to protect personal information under the Data Protection Act 1998 which are appropriate for the different records held whether they are on paper or digitally;

• Ensuring that access to personal information is limited to those on a strictly need to know basis;

• Ensuring that personal information is accurate and up to date;

• Ensuring that personal information is deleted or destroyed as soon as there is no further need for it;

• Ensuring that all employees are trained in their duties and responsibilities under the Data Protection Act, and assess whether they are putting them into practice;

• Ensuring that any notice of breach is reported to the Information Commissioner's Office within 72 hours;

• Ensuring that all personnel are made aware that Exemption 29 under the Data Protection Act can be applied if the police need some information for the prevention and detection of crime or for the apprehension or prosecution of offenders. This exemption cannot be used by the police as a 'fishing exercise', which means that they cannot ask for all records in the hope of catching offenders but must have a specific

request and a need for this information. Only if we are satisfied that the information is going to be used for this purpose and they have given a specific reason for wanting this information can the information be disclosed;

• Ensuring that if we have a legitimate reason for recording calls e.g. for staff training purposes that people are made aware of this;

• For being aware that the Act provides individuals with important rights, including the right to find out what personal information is held on electronic and most paper records;

• For being aware that should an individual or organisation feel they're being denied access to personal information they are entitled to, or feel their information has not been handled according to the eight principles, that they can ask the Information Commissioner to help;

• Ensuring that third party information is removed from computer records before being disclosed;

• Ensuring that manual records which are contained within a ‘’relevant filing system’’ are disclosed on request and that the files which form part of the relevant filing system are structured or referenced in such a way that information about the applicant can be easily located. Where manual files fall within the definition of a relevant filing system, the content will either be sub-divided, which allows the searcher to go straight to the correct category and retrieve the information requested without a manual search, or will be indexed to allow the searcher to go directly to a relevant page(s); and

• Drawing up a Data Security Policy based on the above which is specific to us and ensure that senior management communicate this to everyone within our company. Please refer to our Data Security Policy below.

Everyone within the Firm who processes personal information must comply with the eight principles, which make sure that personal information is:

• Fairly and lawfully processed;

• Processed for limited and specifically stated purposes;

• Used in a way that is adequate, relevant and not excessive;

• Accurate and up to date;

CRBDirect

• Not kept for longer than is necessary;
• Processed in line with individuals' rights;
• Kept safe and secure; and
• Not transferred to other countries without adequate protection.

There is stronger legal protection for more sensitive information which relates to information including:

• ethnic background;
• political opinions;
• religious beliefs;
• health;
• sexual health; and
• criminal records.

Those who process personal information must also:

• Inform the person within the firm who is responsible for Data Protection if a subject access request is made by an individual using their right under the Data Protection Act;
• Ensure that customers are given Customer Documentation which outlines what and how their information is going to be processed. This is to make sure the individual knows exactly what is going to happen to their information and how it is going to be used;
• Not do anything with personal information unless the individual is made aware;
• If a person enquires or wishes to make changes to another customer's agreement you must ask them to ask the customer to send written authorisation showing that they may act for them; and
• Ensure that compliance activities are regularly reviewed to ensure adequate resource and support is being given to these activities.

CRBDirect

CLIENT COMMUNICATION

We communicate with data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Our firm supports the notion of accountability and transparency that are introduced by the General Data Protection Regulation. We will always endeavour to engage our clients with truthfulness and provide full information where we are able to do so. It is our clients who drive the success of our business, and we will handle all personal data with the upmost integrity.