carpenters

Version Control

Version	Name	Reason for change	Approved by	Date
1.0	Angela Coggins	Document Creation	Peter Adlard	07/12/2012
2.0	Maria Rodman	Review and Updated	Maria Rodman	03/01/2014
3.0	Maria Rodman	Updated Breach Reporting	Maria Rodman	19/03/2014
4.0	Maria Rodman	DPA Officer / systems updates	Maria Rodman	05/12/2014

Introduction

Carpenters are required to gather and maintain certain personal data about living individuals for the purposes of satisfying operational and legal obligations.

The Carpenters recognise the importance of the correct and lawful treatment of personal data. The types of personal data that Carpenters may require includes information about: current, past and prospective employees; clients and others with whom it communicates.

This personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the Data Protection Act 1998 and the SRA Code of Conduct 2011.

Carpenters fully endorse and adhere to the eight principles of the Data Protection Act. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation, and storage of personal data. Employees and any others who obtain, handle, process, transport and store personal data for the Carpenters must adhere to these principles.

Principles

The principles require that personal data shall:

1. Be processed fairly and lawfully and shall not be processed unless certain conditions are met;

2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;

3. Be adequate, relevant and not excessive for those purposes;

4. Be accurate and, where necessary, kept up to date;

5. Not be kept for longer than is necessary for that purpose;

6. Be processed in accordance with the data subject's rights;

7. Be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measures;

8. And not be transferred to a country or territory outside 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.

Reporting Breaches

Breaches of our Data Protection Policy or procedures should be reported to the Risk & Compliance Department using the Helpdesk function – risk and compliance breach. You can also speak to your Line Manager or the Risk & Compliance Team directly for an initial discussion and they will advise you whether or not you need to complete an internal Breach Reporting Form.

Subject Access Request

Personal data held by the company and a Clients right to access the data held about them.

 A client has a right to ask what information the Company holds about them and why.

 A right to ask how to gain access to it.

 A right to be informed how to keep it up to date.

 A right to be informed how the company complies with its obligations under the 1998 Data Protection Act.

Rights to Access Information

Employees and other subjects of personal data held by Carpenters have the right to access any personal data that is being kept about them. This is relevant to paper based information and on computer based records. This right is subject to certain exemptions which are set out in the Data Protection Act. Any person who wishes to exercise this right should make the request in writing to the Data Protection Officer, using the standard form. Carpenters aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of a completed form unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

We must provide a client with the relevant data on receipt of the correct form of Subject Access Request. We have a set procedure for complying with a SAR – please contact the Data Protection Officer.

Employee Responsibilities

All employees must ensure that:

 Any personal data they provide to the Company is accurate and up to date

 They inform the Company databases of any changes to information which has been provided, e.g. changes of address, so these can be amended on relevant databases.

 Any information sent out from the company is kept and processed correctly and is accurate and up to date.

 Ensuring all documentation is accurate, relevant and sent to the correct recipient.

If, as part of their responsibilities, employees collect information about other people (e.g.about solicitors practice details or personal circumstances, or about employees in their directorate, clients), they must comply with this Policy and with the guidelines of the 8 Data Protection principles and the Data Protection Act.

Data Security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted to relevant and authorised parties. All staff are responsible for ensuring that any personal data held is kept securely; personal information is not disclosed either orally, in writing or otherwise to any unauthorised third party without consent to do so.

All incoming and outgoing calls that involve client information must go through our Data Protection checks before the claim can be discussed. This relies on checking being made for all incoming and outgoing calls that involve client information. Our checks are system driven and must be followed. If any suspicions are held in the course of undertaking these checks, you must terminate the call. MI is obtained on system DPA.

If a client calls and you do not have access to the system, before discussing the claim, we would request that they provide:

1. Their full address
2. Their date of birth
3. A contact number or email address or occupation.

We must not divulge any information to them, they must give it to us.

If an Insurer calls:

1. The name of the parties
2. The date of the accident
3. Our Clients registration and their insured's registration.

Subject Consent

The need to process data for normal purposes has been communicated to all data subjects. In some cases, if the data is sensitive, for example information about health, race or gender, express consent to process the data must be obtained. Processing may be necessary to operate policies, such as health and safety and equal opportunities.

Retention of Data

Carpenters will keep some forms of information for longer than others according to statutory or regulatory requirements. The company complies with a Data Retention Policy.

Status of the Policy for Clients

Any breach of the Data Protection Policy will be taken seriously and may result in formal action against any member of staff who is found to be negligent in the handling of our Clients personal data. Any breach to data will be fully investigated and reported to any clients affected as soon as possible.

Status of the Policy for employees

Any employee who considers that the policy has not been followed in respect of their own personal data should raise the matter with their Line Manager or the Data Protection Officer in the first instance.

Failure to comply with company policy and procedures may result in disciplinary proceedings against an employee.

Carpenters Designated Data Protection Officer

Carpenters Data Protection Officer is responsible for ensuring compliance with the Data Protection Act and implementation of this policy on behalf of the Partners.

The Data Protection Officer may be contacted as follows:

Mrs. Maria Rodman, Carpenters, Leonard House, Scotts Quays, Birkenhead, CH41 1FB
mro@carpetners-law.co.uk

Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Data Protection Officer.

In Addition

Carpenters Solicitors are accredited with ISO 27001 Data Security Standards of Operation as an additional measure to ensure all data is collated, stored and distributed in a secure manner.