ARC Building Solutions Ltd
PRIVACY POLICY – Customers and Suppliers

Introduction

Purpose

ARC Building Solutions Ltd is committed to being transparent about how it protects personal data and to meeting its data protection obligations. This policy sets out the company's commitment to data protection and individual rights and obligations in relation to personal data.

This policy applies to the private data of our customers and suppliers as well as their employees, workers, apprentices and former employees, and clients.

ARC Building Solutions Ltd has appointed Clair Richardson, Quality & Finance Manager, as the Data Protection Officer. Her role is to inform and advise the company on its data protection obligations. She can be contacted at clair.richardson@arbuildingsolutions.co.uk. Questions about this policy, or requests for further information, should be directed to the Data Protection Officer.

Definitions

"Personal data" is any information that relates to an individual who can be identified from that information alone or in combination with other identifiers the company possesses or can reasonably access. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

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

- lawfully, fairly and in a transparent manner;
- collects personal data only for specified, explicit and legitimate purposes;
- processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing;
- keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay;
- keeps personal data only for the period necessary for processing;
- adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage;
- will not transfer personal data to another country without appropriate safeguards in place;
- will inform its customers the reasons for processing their personal data, how it uses such data and the legal basis for processing in its Privacy Policy. It will not process personal data of individuals for other reasons;
- keeps a record of its processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Individual rights

As a data subject, individuals have several 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 company will inform the individual:

- if 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 EU/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 company has failed to comply with his/her data protection rights; and
- if the company carries out automated decision-making and the logic involved in any such decision-making.

The company 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 the Data Protection Officer. In some cases, the company may need to ask for proof of identification before the request can be processed.

If a subject access request is manifestly unfounded or excessive, the company is not obliged to comply with it. Alternatively, the company 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 company has already responded. If an individual submits a request that is unfounded or excessive, the company will notify him/her that this is the case and if it will respond to it.

Other rights

Individuals have several other rights in relation to their personal data. They can require the company 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 company's legitimate grounds for processing data (where the company 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 if the individual's interests override the company's legitimate grounds for processing data.

To ask the company to take any of these steps, the individual should send the request to Information Security Officer.

In addition, individuals have rights to:

- be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority.

Data security

The company takes the security of personal data seriously. The company 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. The company will regularly evaluate and test the effectiveness of its safeguards to ensure security.

Where the company engages third parties to process personal data on its behalf, such parties do so based on written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and competent measures to ensure the security of data.

Impact assessments

Some of the processing that the company carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the company will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Training

The company will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Data breaches

If the company 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 company will record all data breaches regardless of their effect. If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers

The company will not transfer personal data to countries outside the EEA.

Signed..... N Wolley .....

Date..... 20-1-20 .....

Director:
On behalf of ARC Building Solutions Limited