RETROFITWORKS
BUILDING EFFICIENCY TOGETHER

| | |
|---|---|
| Document title | # Data and Information Sharing Policy |
| Document reference number | # QMS 10 |

*RetrofitWorks Ltd*

# Document particulars:

| | |
|---|---|
| **Document title** | Data and Information Sharing Policy |
| **Document reference number** | QMS 6/10 |
| **Version** | V2 |

| **Version change record:** | | |
|---|---|---|
| **Version** | **Date of issue** | **Description** |
| 1 | 04/01/18 | |
| 2 | 04/01/19 | Take account of new GDPR requirements |
| 3 | | |
| 4 | | |

| | |
|---|---|
| **Directors Name:** | **Russell Smith** |
| **Directors Signature:** |  |
| **Date:** | 04/01/19 |

# Statement of Policy

RetrofitWorks is fully committed to compliance with the requirements of the General Data Protection Regulations (GDPR) set out in the Data Protection Act 2018 ("the Act"), which came into force on the 25th May 2018. The company will therefore follow procedures that aim to ensure that all employees, contractors, consultants, partners or other agents of the company who have access to any personal data held by or on behalf of the company, are fully aware of and abide by their duties and responsibilities under the Act.

# Contents

# Data and Information Sharing Policy

## 1. Introduction

In order to operate efficiently, RetrofitWorks has to collect and use data about people with whom it works. These may include current, past and prospective employees, clients and customers, and suppliers. This personal data must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

RetrofitWorks regards the lawful and correct treatment of personal data as very important to its successful operations and to maintaining confidence between the company and those with whom it carries out business. The company will ensure that it treats personal data lawfully and correctly.

To this end the company fully endorses and adheres to the seven key Principles of Data Protection as set out in Article 5 of the GDPR.

## 2. The principles of data protection

The GDPR sets out **Seven Principles** of good practice. These Principles are legally enforceable.

The Principles require that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
c) ; adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
e) ; kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and

organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

g) The data controller shall be responsible for, and be able to demonstrate compliance with GDPR.

The Act provides conditions for the processing of any personal data. It also makes a distinction between **personal data and special category data**.

Personal data is defined as information relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

Special category data is personal data which the GDPR says is more sensitive, and needs more protection. For example, information about an individual's:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- genetics;
- biometrics;
- health;
- Sexual life or orientation;

# 3. Special Conditions for processing personal data and special category data

First, RetrofitWorks will not collect personal data unless necessary. Specifically, where possible it will seek not to collect personal data for provision of housing analysis services unless required by the client.

RetrofitWorks will, through appropriate management and the use of strict criteria and controls:

- Observe fully conditions regarding the fair collection and use of personal data;
- Meet its legal obligations to specify the purpose for which data is used;

- Collect and process appropriate data and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of data used;
- Apply strict checks to determine the length of time data is held;
- Take appropriate technical and organisational security measures to safeguard personal data;
- Ensure that personal data is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the data is held can be fully exercised under the Act, and respond within the required timeframes

These rights include:

- The right to be informed that processing is being undertaken;
- The right of access to one's personal data The right to prevent processing in certain circumstances;
- The right to, rectify personal data regarded as wrong information, or completed if it is incomplete.
- The right to request erasure of their personal data;
- The right to request restriction or suppression of their personal data
- The right to data portability, to obtain and reuse their personal data for their own purpose across different services
- The right to object to processing of their personal data in certain circumstances, including an absolute right to stop their data being uses for direct marketing

# 4. Accountability and governance

In addition, RetrofitWorks will ensure that:

- There is someone with specific responsibility for data protection in the organisation;
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal data is appropriately trained to do so;
- Everyone managing and handling personal data is appropriately supervised;
- Anyone wanting to make enquiries about handling personal data, whether a member of staff or a member of the public, knows what to do;
- Queries about handling personal data are promptly and courteously dealt with;
- Methods of handling personal data are regularly assessed and evaluated;
- Performance with handling personal data is regularly assessed and evaluated;
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All elected members are to be made fully aware of this policy and of their duties and responsibilities under the Act.

All managers and staff will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
- Individual passwords should be such that they are not easily compromised.

All contractors, consultants, partners or other servants or agents of the company must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the company, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the company and that individual, company, partner or firm;
- Allow data protection audits by the company of data held on its behalf (if requested);
- Indemnify the company against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors who are users of personal data supplied by the company will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by the company.

# 5. Implementation

The company has a designated member of staff with responsibility for data protection who will be responsible for ensuring that the Policy is implemented, and who will also have responsibility for:

- The provision of cascade data protection training, for staff within the company.
- For the development of best practice guidelines.
- For carrying out compliance checks to ensure adherence, throughout the company, with the Data Protection Act.
- Recording any personal data breaches and reporting to the relevant authority and affected individuals if necessary, within the required timeframes.

# 6. Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. RetrofitWorks is registered as such. (https://ico.org.uk/ESDWebPages/Entry/ZA209530)

The Data Protection Act 2018 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis.  Failure to do so is a criminal offence.

To this end the designated officer will be responsible for notifying and updating the designated officer of the processing of personal data.

The designated officer will review the Data Protection Register with designated officers annually, prior to notification to the Information Commissioner.

Any changes to the register must be notified to the Information Commissioner, within 28 days.

RETROFITWORKS

BUILDING EFFICIENCY TOGETHER

RetrofitWorks
Block A, Unit 233
Riverside Business Centre
London SW18 4UQ

Tel: 0330 123 1334
Email: info@retrofitworks.co.uk
Website: www.retrofitworks.co.uk
@retrofitworks