

## Data Handling Policy 2018

### **Introduction**

As part of ever improving services, we are constantly looking for ways to enhance customer experience. Our newest services include electronic contracts. For all contracts we will ask you to provide us with your contact details (sensitive data).

To safeguard our customers with transparency of service, we are requesting your permission to use personal data such as; name, address, telephone number, email address and in certain instances, bank details (appendix A). This document aims to outline our requirement to hold your data, sensitively, confidentially and with integrity.

### **Policy Statement**

#### **1.1 Scope**

To ensure that we handle your data responsibly, we will ask for your consent to store and share your details in the following ways:

- Hold personal information for a period up to and including 10 years, in conjunction with the guarantee period | after such time data will be moved to encrypted files
- Share details with contractors and sub-contractors, installers, suppliers, insurers and professional governing bodies such as FENSA, GGF and GGF.i.
- Personal data will be used to contact customers during the enquiry, quotation, installation stages, help us store and file customers for reference and future work.

#### **1.2 Information Access**

You have the right to request access to free copies of any and all information we hold of you. If we deem your requested to be manifestly unfounded or unreasonable, we may ask for a fee to cover administration costs.

#### **1.3 Classification of Information**

All information held will either be locked in storage or password protected. Where information is shared with a third party, such as a contractor, the policy of the company handling the data will supersede our own.

#### **1.4 Marketing & Out of Contract Communications**

Stratton Glass and Windows Ltd does not participate in any direct marketing unless agreed. We will not contact you, nor share your details with anyone, for any of the following reasons:

- Direct Sales
- Promotions
- Surveys & Feedback

## 1.5 Destroying Data

We will readily destroy any and all unnecessary data held. Physical data will be shredded onsite, immediately, at the moment of obsolescence. Electronic data will be deleted in accordance with our archiving procedures.

## 1.6 Data Breaches

We currently have a range of software packages designed to help us process data. Each data handler is given security clearance depending on the company hierarchy. Each stage of data access as well as each system, requires individual login and password details.

We take electronic security very seriously. We regularly update both hardware and software packages. We currently operate both sites through a fibre-optic link. Our software, including firewall, is supported remotely by a company called SEDCOM. We have the ability to remotely shut-down all systems.

## 1.7 Consent

Due to the bespoke nature of the work, contracts are agreed upon using quotations. To proceed with a contract we require your consent. This may be a signed carbon copy contract form, an email agreement or verbal consent. All paper consent forms and emails will be kept on file for the duration of the guarantee period. These will be for any job over the value of £42.00 inc. VAT. Verbal consent can only be done over the phone for a value less than this. The telephone recording will be held for a period of 3 months, where express consent to proceed is given.

## 1.8 Archiving

After a period of 3 years, data on software packages will be transposed to hard copies and archived using a numeric coding system. This will be kept in a locked storage facility to be accessed in the event of the guarantee coming into force.

Sensitive data will be routinely backed up for storage purposes to ensure data corruption does not impact on current workloads.

Financial software will hold data indefinitely. This is for:

- Value Added Tax Auditing
- Internal account checking

The data within the software is 'hidden', meaning that all sensitive information is redacted.

## 1.9 Right to Erasure

Under new legislation GDPR, you have the right to be forgotten. This means that you can request that we delete all data we hold of you if; we no longer require the data (such as the contract term ending), you withdraw consent (see cancellations), we have processed your data illegally or outside the scope of its intended delivery. This must be a written request, time appropriate i.e. if you wish for data to be deleted after we no longer require it you will have to request at the end of the 10 year term.