

Certainfil Cavity Insulation Limited

Data Protection Statement (GDPR):

Scope

This Statement details how we collect, keep and use personal data. It should be read in conjunction with our Data Protection Policy

Purpose

To ensure transparency in accordance with Data Protection regulations (GDPR).

What Data do we collect, keep and use?

The name, address, telephone number and e-mail address (if provided) for each client and details of the property on which we will be carrying out works.

For the purposes of providing grant funding we may record date of birth and general income details i.e. is the income below a specified threshold but not specific income amounts.

How do we use this Data?

We use the data collected to:

- Survey and ensure the proposed works can be carried out in accordance with current regulations and accreditation requirements.
- Facilitate the installation of insulation measures requested by the client
- Facilitate the grant application process and subsequent funds release
- Arrange post installation inspections to meet regulatory and accreditation requirements
- Facilitate the financial accounting processes required in accordance with current Legislation.
- Facilitate the issue of guarantees for works completed where appropriate.

Who do we share your data with?

- Our Installers – to enable the installation of requested works.
- Funding Bodies and Programme Administrators in relation to grant funded works in pursuit of the claim.
- National and Local Government agencies in accordance with statutory or regulatory duties associated with proper conduct of lawful business i.e. HMRC and Building control in accordance with current regulation.
- Our Accreditation Body: to facilitate randomised inspection and assessment of works for the purposes of quality control and compliance with assurance standards.
- Third party insurance provider in respect of the 25year guarantee provided for Cavity Wall Insulation
- Our Data is also provided to our Accountant for the purposes of filing returns in accordance with Companies Act and HMRC regulations.

How and when we contact you

- We will contact you by phone, e-mail, SMS or in writing for the following reasons:
- In response to a request for quotation
- In order to confirm details associated with your order or application for grant funding
- In order to schedule proposed works following placement of an order
- To follow up on any post installation inspection requirements
- To follow up on payment issues

You may be contacted directly by our Accreditation Body or the Grant Scheme Administrators who carry out randomised inspections of our work for the purposes of quality control.

Data Retention

We will hold your data for a period up to 25 years. In order to provide you with a 25 year guarantee we must retain the data relating to the installation of your insulation. We must retain the details of your property for

the purposes of providing traceability of the products used, the methods of installation and the suitability of the property at the time of installation.

Data obtained and processed in relation to grant funding must be held for a period of 7 years in accordance with the funding provider requirements.

Your rights

You have the following rights regarding your personal data:

Rights	What does this mean:
1. Right to be informed	You have the right to be provided with clear, transparent and easily understandable information about how we use your personal data and your rights. This is why we are providing you with the information in this Privacy Policy.
2. Right of access	You have the right to obtain access to your personal data (if we are processing it) and certain other information (similar to that provided in this Privacy Policy). This is so you are aware and can check that we are using your personal data in accordance with data protection law.
3. Right to rectification	You are entitled to have your personal data corrected if it is inaccurate or incomplete.
4. Right to erasure	This is also known as 'the right to be forgotten' and, in simple terms, enables you to request the deletion or removal of your personal data where there is no compelling reason for us to keep using it. This is not a general right to erasure; there are exceptions.
5. Right to restrict processing	You have the right to 'block' or suppress further use of your personal data in certain circumstances. When processing is restricted, we can still store your personal data, but may not use it further. We keep lists of people who have asked for further use of their personal data to be 'blocked' to make sure the restriction is respected in future.
6. Right to data portability	You have the right to obtain and reuse your personal data in a structured, commonly used and machine-readable format in certain circumstances. In addition, where certain conditions apply, you have the right to have such information transferred directly to a third party.
7. Right to object to processing	You have the right to object to us processing your personal data for our legitimate business interests.
8. Right to withdraw consent to processing	If you have given your consent to us to process your personal data for a particular purpose (for example, to survey your property), you have the right to withdraw your consent at any time (although if you do so, it does not mean that any processing of your personal data up to that point is unlawful).
9. Right to make a complaint to the data protection authorities	You have the right to make a complaint to the Information Commissioner's Office (ICO) if you are unhappy with how we have handled your personal data or believe our processing of your personal data does not comply with data protection law.

Contacting us

If you wish to contact us regarding your Data please do so in writing, we will review your request and respond within one month.

Data Protection Policy

Certainfil Cavity Insulation Limited

Last updated	30 April 2019
--------------	---------------

Definitions

Comapny	means Certainfil Cavity Insulation Limited a registered Comapny.
GDPR	means the General Data Protection Regulation.
Responsible Person	means Annetta McCullough, Director
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Comapny.

1. Data protection principles

The Comapny is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

- a. processed lawfully, fairly and in a transparent manner in relation to individuals;
- 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;
- c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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;
- 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; and
- 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.”

2. General provisions

- a. This policy applies to all personal data processed by the Comapny.

- b. The Responsible Person shall take responsibility for the Company's ongoing compliance with this policy.
- c. This policy shall be reviewed at least annually.
- d. The Company shall register with the Information Commissioner's Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

- a. To ensure its processing of data is lawful, fair and transparent, the Company shall maintain a Register of Systems.
- b. The Register of Systems shall be reviewed at least annually.
- c. Individuals have the right to access their personal data and any such requests made to the Company shall be dealt with in a timely manner.

4. Lawful purposes

- a. All data processed by the Company must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests ([see ICO guidance for more information](#)).
- b. The Company shall note the appropriate lawful basis in the Register of Systems.
- c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Company's systems.

5. Data minimisation

- a. The Company shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

- a. The Company shall take reasonable steps to ensure personal data is accurate.
- b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

- a. To ensure that personal data is kept for no longer than necessary, the Company shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
- b. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

- a. The Company shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
- b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- c. When personal data is deleted this should be done safely such that the data is irrecoverable.
- d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Company shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO ([more information on the ICO website](#)).

END OF POLICY