Data Protection Policy and General Data Protection Regulations (GDPR) Compliance

Data Protection Policy and Procedures

Introduction

Cistermiser Ltd / Keraflo Ltd (Cistermiser Keraflo) are fully-owned subsidiaries of Davidson Holdings Ltd.

We are committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of data in order to carry out our work. This personal information must be collected and dealt with appropriately. The Data Protection Act 1998 (DPA) governs the use of information about people (personal data). Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographic images.

Cistermiser Keraflo will remain the Data Controller for the information held. The Directors and staff will be personally responsible for processing and using personal information in accordance with the Data Protection Act. Directors and staff who have access to personal information, will be expected to read and comply with this policy at all times.

Purpose

The purpose of this policy is to set out our commitment and procedures for protecting personal data at Cistermiser Keraflo. The Board of Directors regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal with.

The Data Protection Act

This contains 8 principles for processing personal data with which we must comply at all times.

Personal data:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,

2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,

3. Shall be adequate, relevant and not excessive in relation to those purpose(s),

4. Shall be accurate and, where necessary, kept up to date,

5. Shall not be kept for longer than is necessary,

6. Shall be processed in accordance with the rights of data subjects under the Act,

7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,

8. Shall 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 information.

Definitions

The following list contains definitions of the technical terms we have used and is intended to aid understanding of this policy:

Data Controller – This is the person who (either alone or with others) decides what personal information Cistermiser Keraflo will hold and how it will be held or used.

Data Protection Act 1998 – This is the UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – This is the person on the senior management team who is responsible for ensuring that it follows its data protection policy and complies with the Data Protection Act 1998.

Data Subject/Service User – This is the individual whose personal information is being held or processed by Cistermiser Keraflo.

'Explicit' consent – This is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing of personal information about her/him. Explicit consent is needed for processing sensitive data that includes the following:

(a) Racial or ethnic origin of the data subject

(b) Political opinions

(c) Religious beliefs or other beliefs of a similar nature

(d) Trade union membership

(e) Physical or mental health or condition

(f) Sexual orientation

(g) Criminal record

(h) Proceedings for any offence committed or alleged to have been committed.

Notification – This means notifying the Information Commissioners Office (ICO) about the data processing activities of Cistermiser Keraflo.

Information Commissioner – This is the UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing – This means collecting, amending, handling, storing or disclosing personal information.

Personal Information – This is specific information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual customers who have purchased Cistermiser Keraflo products (e.g. self-employed installers and homeowners).

Applying the Data Protection Act within Cistermiser Keraflo

Access to Personal Information

Access is limited to Directors and staff who may undertake tasks which involve the collection of personal details from members of the public. In such circumstances, we will let people know why we are collecting their data and it is our responsibility to ensure the data is only used for this purpose.

Correcting data

Individuals have a right to have data corrected if it is wrong, to prevent use which is causing them damage or distress, or to stop marketing information being sent to them.

Responsibilities

Cistermiser Keraflo is the Data Controller under the Act, and is legally responsible for complying with Act, which means that it determines what purposes personal information held will be used for.

The Directors and senior management team at Cistermiser Keraflo will take into account legal requirements and ensure that the Act is properly implemented and, through appropriate management, ensure strict application of criteria and controls.

The Data Controller will at all times:

a) Observe fully conditions regarding the fair collection and use of information.

b) Meet its legal obligations to specify the purposes for which information is used.

c) Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.

d) Ensure the quality of information used.

e) Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:

i) The right to be informed that processing is being undertaken.

ii) The right of access to one's personal information.

iii) The right to prevent processing in certain circumstances.

iv) The right to correct, rectify, block or erase information which is regarded as wrong information.

f) Take appropriate technical and organisational security measures to safeguard personal information.

g) Ensure that personal information is not transferred abroad without suitable safeguards.

h) Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.

i) Set out clear procedures for responding to requests for information.

Data Protection Officer

The Data Protection Officer sits on the Board of Directors of Davidson Holdings Ltd (i.e. the parent company of Cistermiser Keraflo) and is identified as:

Name: Stuart Johnson, Financial Director, Davidson Holdings Ltd

Registered Office: Unit 1, Woodley Park Estate, 59-69 Reading Road, Woodley, Berkshire, RG5 3AN

The Data Protection Officer will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

a) Ensuring that everyone processing personal information understands that they are contractually responsible for following good data protection practice.

b) Ensuring that everyone processing personal information is appropriately trained to do so.

c) Ensuring that everyone processing personal information is appropriately supervised.

d) Ensuring that anybody wanting to make enquiries about handling personal information knows what to do.

e) Ensuring that any enquiries about handling personal information are dealt with promptly and courteously.

f) Describing clearly how the business handles personal information.

g) Regularly reviewing and auditing the ways that Cistermiser Keraflo holds, manages and uses personal information.

h) Regularly assessing and evaluating Cistermiser Keraflo's methods and performance in relation to handling personal information.

All Directors and staff at Cistermiser Keraflo are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

In case of any queries or questions in relation to this policy, please contact the Data Protection Officer.

Data collection: Informed consent

Informed consent is when a Data Subject clearly understands why their information is needed; who it will be shared with; the possible consequences of them agreeing or refusing the proposed use of the data; and then gives their consent.

We will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form. When collecting data, we will ensure that the Data Subject:

a) Clearly understands why the information is needed.

b) Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing.

c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed.

d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress.

e) Has received sufficient information on why their data is needed and how it will be used.

Procedures for Handling Data & Data Security

Under the Data Protection Act 1998, companies have a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

- Unauthorised or unlawful processing of personal data.
- Unauthorised disclosure of personal data.
- Accidental loss of personal data.

All staff must therefore ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper or in a computer or recorded by some other means.

Personal data relates to data of living individuals who can be identified from that data and use of that data could cause an individual damage or distress. This does not mean that mentioning someone's name in a document comprises personal data; however, combining various data elements such as a person's name and salary or religious beliefs, etc. would be classed as personal data, and falls within the scope of the Data Protection Act.

It is therefore important the all staff consider any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data and observe the guidance given below.

Operational Guidance for Cistermiser Keraflo Staff

Email: All staff should consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained it should be saved into the appropriate folder

or, printed and stored securely. The original email should then be deleted from the personal mailbox and any "deleted items" box, either immediately or when it has ceased to be of use. Emails that contain personal information which is no longer required for operational use, should be deleted from the personal mailbox and any "deleted items" box.

Phone Calls: Incoming phone calls from 3rd parties can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

- If you receive a phone call asking for personal information to be checked or confirmed, be aware that the phone call may come from someone pretending to be the data subject, or impersonating someone with a right of access.
- Personal information should not be given out over the telephone unless you have no doubts as the caller's identity and the information requested is innocuous. If you have any doubts, ask the caller to put their enquiry in writing.

Laptops and Portable Devices: All laptops and portable devices that hold data containing personal information must be protected with a suitable encryption program. Ensure your laptop is locked (password protect) when left unattended, even for short periods of time. When travelling in a car, make sure the laptop is out of site, preferably in the boot. If you have to leave your laptop in an unattended vehicle at any time, put it in the boot and ensure all doors are locked and any alarm set. Never leave laptops or portable devices in your vehicle overnight. Do not leave laptops or portable devices unattended in restaurants or bars, or any other venue. When travelling on public transport, keep it with you at all times, do not leave it in luggage racks or even on the floor alongside you.

Data Security and Storage: Store as little personal data as possible on your computer or laptop; only keep those files that are essential. Personal data received on disk or memory stick should be saved to the relevant file on the server or laptop. The disk or memory stick should then be securely returned (if applicable) or processed for safe storage or disposal. Always lock (password protect) your computer or laptop when left unattended; this is especially important when using your laptop away from the office.

Passwords: Do not use passwords that are easy to guess. Make sure all of your passwords contain both upper and lower-case letters and preferably contain some numbers. Ideally passwords should be 6 characters or more in length.

Protect Your Password: Common sense rules for passwords are:

- Do not give out your password.
- Do not write your password somewhere on your laptop.
- Do not keep it written on something stored in the laptop case.

Data Storage Information and records relating to Cistermiser Keraflo product purchases, product warranty registrations and product warranty claims will be stored securely and will only be accessible to authorised Directors and staff.

Information will be stored for only as long as it is needed or required for statutory purposes and will be disposed of appropriately.

It is our responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on or sold to a third party. This policy will be updated as necessary to reflect best practice in data management,

security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

Information Regarding Employees or Former Employees

Information regarding an employee or a former employee may be kept indefinitely in a secure location. Cistermiser Keraflo might have a need to refer back to a job application or other document to check specific details relevant to the former term of employment.

Data Subject Access Requests

Members of the public may request certain information under the Freedom of Information Act 2000. Cistermiser Keraflo will respond to requests for information under the Data Protection laws.

Disclosure

We may need to share data with other external agencies such as approved and carefully vetted third party postal mail printing and fulfilment partners. We regard the lawful and correct treatment of personal information as very important to successful working and to maintaining the confidence of those with whom we deal. We will ensure that personal information is treated lawfully and correctly at all times.

Risk Management

The consequences of breaching Data Protection can cause harm or distress to customers and former employees if their information is released to inappropriate people. Directors and staff should be aware that they can be personally liable if they use customers' or former employees' personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of Cistermiser Keraflo is not damaged through inappropriate or unauthorised access and sharing.

Destroying personal data

Personal data should only be kept for as long as it is needed i.e. data will be kept for the duration of administering product purchases and warranty registrations and securely disposed of as appropriate once the processing period is complete. We will review personal data annually, and will ensure that this information is confidentially destroyed at the end of the relevant retention period.

Further information

If members of the public or stakeholders have specific questions about information security and data protection in relation to Cistermiser Keraflo, please contact the Data Protection Officer. The Information Commissioner's website (www.ico.gov.uk) is another source of useful information.

The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) comes into force in the UK from 25th May 2018. The UK Government has confirmed that Brexit will not affect the implementation of the GDPR. The proposed European Union (Withdrawal) Bill (also referred to as the "Great Repeal Bill") means it is likely to be converted into British Law.

The GDPR is applied to organisations that are either controllers of the data or those processing the data. As outlined in the current Data Protection Act (DPA), a controller is responsible for how and why personal data is processed and a processor is responsible to act on the controller's behalf. However, in the GDPR the processor now has a specific legal obligation to maintain records on what personal data they are processing and the processing activities. Therefore, under GDPR both the controller and processor now have defined legal responsibilities.

In the GDPR, personal data has been redefined and is now covers a much wider scope, including new areas such as IP addresses, CCTV, biometrics. The GDPR also covers a 'special category of personal data, referred to as sensitive data and may only be processed only within a limited number of circumstances. The principles that underpin GDPR are ones that we would all hope that people will carry out with our own data.

GDPR Article 5 states that personal data shall be (paraphrased):

a) Processed lawfully, fairly and in a transparent manner;

b) Collected for specified, explicit and legitimate purposes;

c) Adequate, relevant and limited to what is necessary;

d) Accurate and, where necessary, kept up to date;

e) Kept for no longer than is necessary;

f) Processed in a manner that ensures appropriate security of the personal data.

These principles encapsulate some very important new requirements. For example, consent must be "informed consent", i.e. the information on which the consent was given is informative, unambiguous, and is given freely. In addition, consent can be withdrawn. Data relating to children (under 16) requires authorisation from a parent or guardian, and the controller is to make all reasonable efforts to obtain this.

A number of rights of the individual are now defined and enforced in GDPR:

1. Right to be informed: businesses must provide 'fair processing information'.

2. Right to access: confirmation that their data is being processed; access to their personal data; and other supplementary information.

3. Right to rectification: people can correct incorrect information.

4. Right to erasure: that is to be forgotten.

5. Right to restriction of processing: data can be stored but not processed.

6. Right to portability: to take and reuse their personal data across a range of services.

7. Right to object.

8. Right to decision making: people can object if a human being is not involved in a decision made about their data.

As part of the GDPR, Cistermiser Keraflo must provide a Data Protection Impact Assessment (DPIA). The DPIA identifies the specific risks to personal data as a result of processing activity and must be undertaken whenever there is a change in processes, technology, or new activity within the business.

In addition, there are two interrelated processes required for the implementation of GDPR:

1. Design of systems and processes which secure the data.

2. Design of systems and processes, which ensure that data is managed properly.

Applying the GDPR within Cistermiser Keraflo

Data Protection Impact Assessment (DPIA)

We have identified all personal information data currently processed by Cistermiser Keraflo and carried out an impact risk assessment for each set of data.

The majority of customer records held on our Sage CRM and Sage 200 operating systems relate to business to business (B2B) customer purchase transactions, including corporate business addresses and email/telephone contact information. Financial transaction details are held for 7 years, in accordance with statutory requirements.

However, in addition to business to business (B2B) customers our Combimate limescale prevention unit and associated Combiphos annual refill products are also sold to business to consumer (B2C) customers, i.e. members of the public including homeowners and self-employed professional installers who submit personal information including home addresses to register their product purchases and secure extended warranty status.

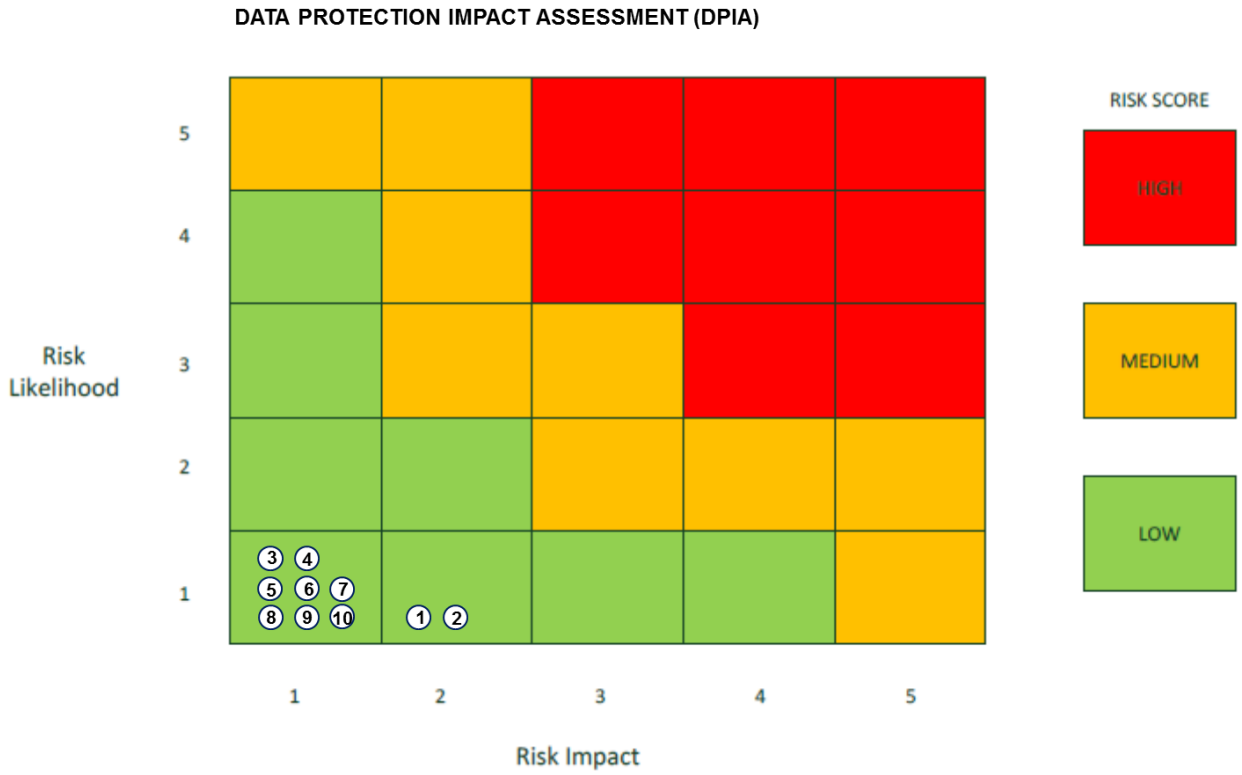
Cistermiser Keraflo has updated systems and processes for both securing and then managing Combimate/Combiphos customer data as outlined below, to ensure GDPR-compliant procedures are followed at all times.

Personal information lawfully held at Cistermiser Keraflo is defined as follows:

1. Combimate limescale prevention unit product registrations to apply for extended warranty status (3 years or lifetime guarantee options)
2. Combiphos annual refill purchase registrations to maintain extended warranty status for Combimate product installations (3 years or lifetime guarantee options)
3. Credit card details for PayPal purchases processed via our online Sage 200 portal
4. Credit card details for telephone purchases processed using a hand-held machine at our Woodley office (Keraflo Spares)
5. Customer details relating to Technical Support queries (including Combimate)
6. Customer details relating to faulty goods or product returns enquiries (including Combimate)
7. Payroll bank account details for current employees
8. HR personal file records for current employees
9. HR personal file records for ex-employees

10. HR personal information for unsuccessful job applicants

Impact risk assessment status for personal information held at Cistermiser Keraflo is summarised as follows:



Impact risk assessment notes for personal information held at Cistermiser Keraflo:

1. Combimate limescale prevention unit product registrations – These are a key focus for GDPR compliance. Design of systems and process disciplines for managing this data are detailed below.
2. Combiphos annual refill purchase registrations – These are a key focus for GDPR compliance. Design of systems and process disciplines for managing this data are detailed below.
3. Credit card details for PayPal purchases – Payments are processed in accordance with the Information Commissioner's Office (ICO), Payment Card Industry Data Security Standard (PCI DSS) and Financial Services Compensation Scheme (FSCS) regulated standards.
4. Credit card details for telephone purchases – Payments are processed in accordance with the Information Commissioner's Office (ICO), Payment Card Industry Data Security Standard (PCI DSS) and Financial Services Compensation Scheme (FSCS) regulated standards. Handwritten notes taken over the telephone are shredded on the same day as payments are processed.
5. Customer details relating to Technical Support queries – Brief identification details are retained after queries are processed, to ensure traceability if required.
6. Customer details relating to faulty goods or product returns enquiries – Brief identification details are retained after enquiries are processed, to ensure traceability if required.
7. Payroll bank account details for current employees – This data is securely managed by the Finance Director only, with administrative back-up provided by the Data Protection Officer. Information protected by unique payroll ID is shared with HMRC as required and Cistermiser Keraflo also fully complies with ONS information requests.

8. HR personal file records for current employees – Consent to hold personal information is obtained from employees as a standard discipline. Line Managers are instructed to dispose of document copies containing elements of employee personal data (e.g. home addresses) that may be held in their office files. Cistermiser Keraflo's recorded Health & Safety Accident Report documentation no longer includes any reference to employee home addresses. Disciplinary procedure details are retained in accordance with statutory requirements, then deleted.
9. HR personal file records for ex-employees – This information including exit interview notes is held securely in an archive vault, with restricted access only by Directors.
10. HR personal information for unsuccessful job applicants – These are shredded/deleted as soon as possible once the recruitment process has been completed.

Restricted elements of personal information lawfully held at Cistermiser Keraflo are shared with external agencies who provide specialist third party services, as follows:

- **Besley & Copp** – Combiphos refill annual purchase reminder postal letters are sent every year as requested to UK homeowner or self-employed professional installer home addresses via a service managed by our fulfilment partners Besley & Copp. Responding to our audit request, this company has provided Cistermiser Keraflo with a written assurance to confirm the integrity of their data management procedures. Besley & Copp's Privacy Policy can be viewed online at www.besleyandcopp.co.uk and a transcript copy is available on request.
- **PayPal** – Purchases made online by credit card are processed using PayPal Services. The Privacy policy for PayPal Services can be viewed and downloaded online at www.paypal.com and a pdf copy is available on request.
- **Textlocal** – Online PayPal purchase customers, callers requesting Technical Support assistance and customers who have made a faulty goods or product return enquiry logged on our Sage CRM system are sent SMS text messages requesting a Customer Satisfaction rating of our services via Textlocal's Messenger 3.0 platform. Every text sent by Cistermiser Keraflo using Textlocal Messenger includes an option for recipients to opt-out from SMS text messages. Textlocal's Privacy Policy and Legal Compliance statements can be viewed online at www.textlocal.com and transcript copies are available on request.

Design of Systems and Processes for implementation of GDPR

The GDPR legislation has provided an opportunity for Cistermiser Keraflo to tighten up operational processes relating to the deletion of information when no longer required and also to improve the transparency and communication of our data protection policy and procedures.

The Combimate Installation Guide has been redesigned to update the freepost application form completed by UK homeowners and self-employed professional installers when registering their product purchases to secure extended warranty status.

This form now includes "opt-in" consent tick boxes for two services offered by Cistermiser Keraflo:

- consent to receive annual Combiphos refill reminders via post or email (Homeowners)
- consent to receive trade news updates (an option for Installers only)

PLEASE USE BLOCK CAPITALS

Serial No. ..... Date Installed .....
(on the side of the base, once the cover is removed)
Protection selected (tick one): ☐ Complete supply or ☐ Single appliance

Make and model of boiler..... Approx. age .....

Yes, I wish to receive an annual Combiphos reminder, to be sent by:
☐ **Post** (tick one)
☐ **Email** (tick one)

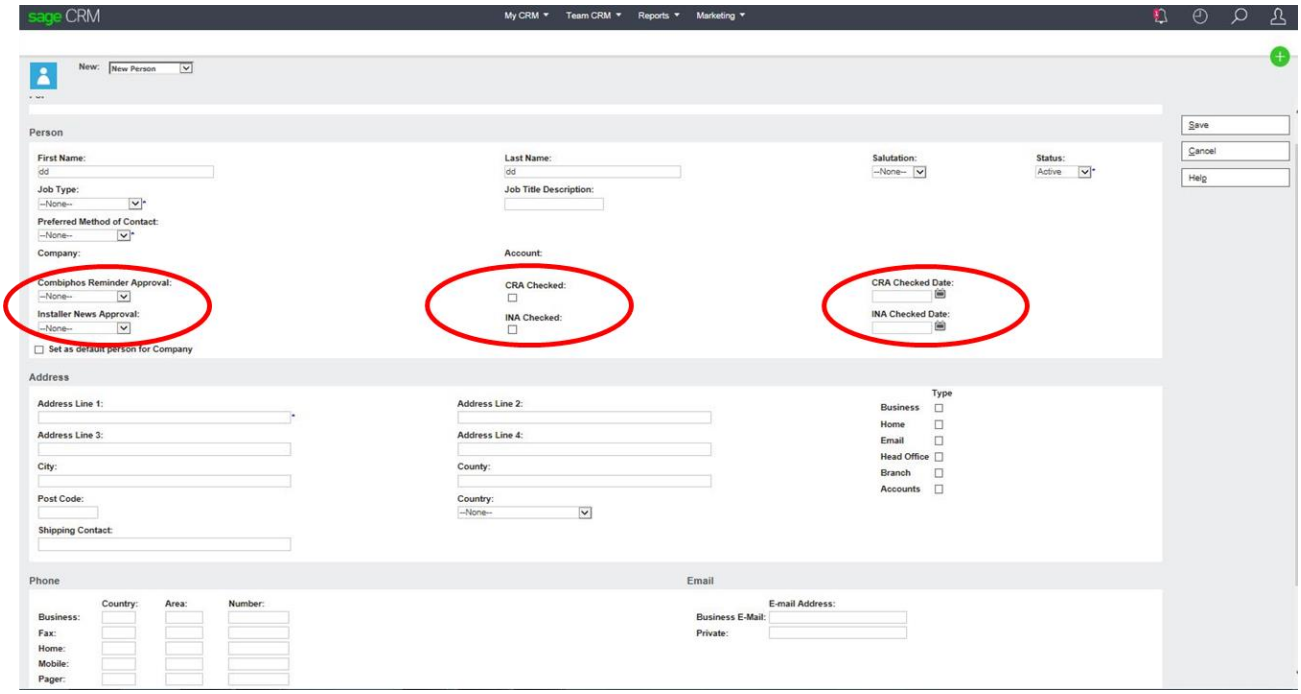
OPTIONAL - TO APPLY FOR THE LIFETIME SCALE PREVENTION GUARANTEE, PLEASE INCLUDE:
☐ New boiler installation receipt (tick one)
☐ New heat exchanger installion receipt (tick one)

Name and address of Homeowner: .....
.....
.....
.....
Post Code ..... Email .....
Signed .....

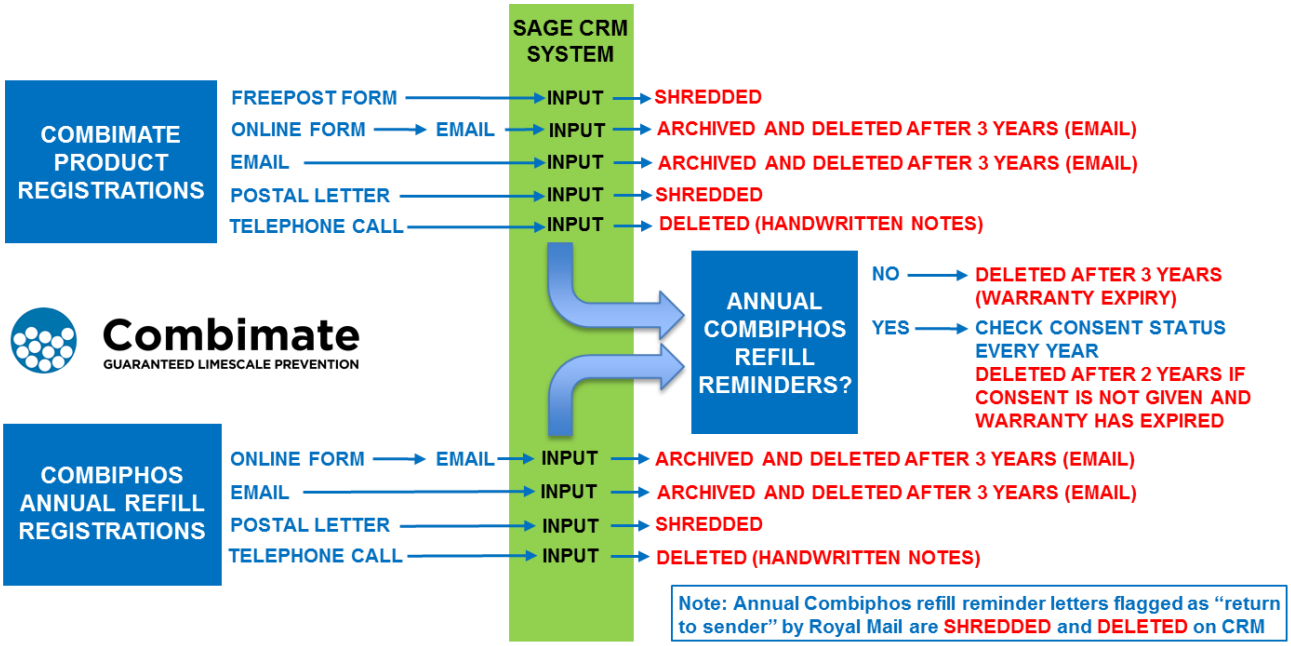
OPTIONAL - TO BE COMPLETED BY THE INSTALLER:
Yes, I wish to receive trade news updates about Combimate and Cistermiser's associated water-saving products to be sent by:
☐ **Post** (tick one)
☐ **Email** (tick one)
Name and address of installer: .....
.....
.....
Post Code ..... Email .....

The online version of this Combimate registration form has also been redesigned to include "opt-in" consent approval.

Our Sage CRM system has been redesigned to log appropriate "opt-in" consent status for annual Combiphos reminders and Installer News updates in specific fields. Additional new fields have been added to enable checking of consent approval status and logging of associated dates.



Our data management strategy for Combimate and Combiphos registrations includes the deletion of personal data records when no longer required (for extended warranty or lifetime scale prevention guarantee purposes) and is summarised as follows:



Personal information processed by Cistermiser Keraflo will always be used fairly, stored safely and never disclosed unlawfully.

We are committed to the fundamental principle embedded in legislation that personal information will be managed consistently and appropriately at all times, to ensure GDPR compliance.