

1. Secure Processing

The Company shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the data protection and organisational measures that shall be taken are provided in Parts 7 and 8 of this Policy.

2. Data Portability

- a) The Company processes personal data using automated means. NetSuite ERP, Sage, Email address book, spreadsheets, GV, Phones
- a) Where data subjects have given their consent to the Company to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations).
- b) To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following format: Email.
- b) Where technically feasible, if requested by a data subject, personal data shall be sent directly to another data controller.
- c) All requests for copies of personal data shall be complied with within **one month of the data subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests and in such cases the data subject shall be informed of the need for the extension).**

3. Personal Data Held

The following personal data may be collected, held, and processed by the Company:

- a) Personal name and address, personal phone numbers and personal email address.
- b) Company name and address, company personal phone numbers and company email address.

4. Data Protection Measures

A. The Company shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

- a) All internal emails containing personal data must be encrypted by copying and pasting the link to the NetSuite Record.
- b) Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely.
- c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- d) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- f) Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- g) Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using recorded delivery.
- h) No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to; such access should be formally requested from the DPO.
- i) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;
- j) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the DPO.
- k) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;
- l) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
- m) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Company or otherwise without formal written approval of the DPO and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.
- n) No personal data should be transferred to any device personally belonging

to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);

- o) All personal data stored electronically should be backed up monthly with back-ups stored onsite. All backups should be encrypted using industry standard pass-wording;
- p) All electronic copies of personal data should be stored securely using passwords and data encryption;
- q) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by the Company is designed to require such passwords;
- r) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
- s) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the DPO to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service. Such details should be checked at least annually.

5. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- a) All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual **responsibilities and the Company's responsibilities under the Regulation** and under this Policy, and shall be provided with a copy of this Policy;
- b) Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;
- c) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
- d) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;

- e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;
- f) The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- g) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;
- h) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation;
- i) Where any agent, contractor, or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims, or proceedings that may arise out of that failure.

A.1. General

This Policy sets out the privacy controls of Thermogroup Ltd T/A ThermoSphere (**"the Company"**) regarding data protection and the rights of *customers, suppliers, employees, business contacts, etc.* (**"Data subjects"**) in respect of their personal data under the **General Data Protection Regulation ("the Regulation")**. Other aspects of the Regulations are met by the Company's information security controls.

The Regulation defines **"personal data"** as any information relating to an identified or identifiable natural person (a data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy shall be deemed effective as of 01st March 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Nigel Dowding

Position: Data Protection Officer

Last Review Date : 01st March 2018

Due for Review by: 01st March 2019

A..2 General policies for the use and protection of personal data

This Policy sets out the procedures that are to be followed when dealing with personal data. All employees, agents, contractors, or other parties working on behalf of the Company must follow the procedures and principles set out herein all times.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

The regulation sets out seven key principles that lie at the heart of the **company's approach to processing personal data.**

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

A.3.1 Consent

Personal data may be processed where the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

A.3.2 Choice

- c) In the event that the Company uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Company.
- d) The right described in Part H1-a does not apply in the following circumstances:
- e) The decision is necessary for the entry into, or performance of, a contract between the Company and the data subject;
- f) The decision is authorised by law; or
- g) The data subject has given their explicit consent.
- h)
- i)

Right To Object

- a) Data subjects have the right to object to the Company processing their personal data based on legitimate interests (including

profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

- b) Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing forthwith, unless it can be demonstrated that **the Company's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.**
- c) Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing forthwith.
- d) Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, **'demonstrate grounds relating to his or her particular situation'**. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

Right to Request Data Processing to stop

- a) Data subjects may request that the Company stops processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.
- b) In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

Automated Decision making

- a) In the event that the Company uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Company.
- b) The right described in Part a does not apply in the following circumstances:
 - I. The decision is necessary for the entry into, or performance of, a contract between the Company and the data subject;
 - II. The decision is authorised by law; or
 - III. The data subject has given their explicit consent.

Profiling

- a) Where the Company uses personal data for profiling purposes, the following shall apply:

- b) Clear information explaining the profiling will be provided, including its significance and the likely consequences;
- c) Appropriate mathematical or statistical procedures will be used;
- d) Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and

All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 7 and 8 of this Policy for more details on data security).

A.4.1 Purpose Legitimacy

Personal data processing other than consent shall be based on one of the following grounds:

- a. Processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- b. Processing is necessary for compliance with a legal obligation to which the controller is subject;
- c. Processing is necessary to protect the vital interests of the data subject or of another natural person;
- d. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- e. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject that require protection of personal data, in particular where the data subject is a child.

A.4.2 Purpose Specification

The Company shall ensure that the following information is provided to every data subject when personal data is collected:

- b) Details of the Company including, but not limited to, the identity of the DPO its Data Protection Officer;
- c) The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 6 of this Policy) and the legal basis justifying that collection and processing;
- d) Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;
- e) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- f) Where the personal data is to be transferred to one or more third parties, details of those parties;
- g) Where the personal data is to be transferred to a third party that is **located outside of the European Economic Area (the "EEA"), details of**

that transfer, including but not limited to the safeguards in place (see Part A.13.2 of this Policy for further details concerning such third country data transfers);

- h) Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined);
- i) **Details of the data subject’s rights under the Regulation;**
- j) **Details of the data subject’s right to withdraw their consent to the Company’s processing of their personal data at any time;**
- k) **Details of the data subject’s right to complain to the Information Commissioner’s Office (the ‘supervisory authority’ under the Regulation);**
- l) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;
- m) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

The table below shows when the information in Part A.4.2 shall be provided to the data subject.

Source or Destination of Personal Data	Disclosure Date
Obtained directly from the data subject	At the time of collection
Obtained from Third Party	At the time of collection
Used to communicate with Data Subject	At time of first communication
To be disclosed to Third Party	Before Disclosure
In any event	Not more than one month after the data is obtained

A.5 Collection Limitation

- a) The Company collects and processes the personal data set out in Part 6 of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us) and data received from third parties (for example, customer referrals, trade enquiries, ABI /Glenigan, recruitment companies).
- n) The Company only processes personal data for the specific purposes set out in Part A.4.1 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or

as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

- o) 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.

A.6 Data Minimization

A.7.1. Use, Retention and Disclosure Limitation

- a. The Company will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part A.4.2., above
- b. The Company shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it immediately.

A.8. Accuracy and Quality

- a) The Company shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken immediately to amend or erase that data, as appropriate.

A.9.1 Privacy notice

A.9.2 Openness and transparency

The Company's data protection officer ("DPO") is Nigel Dowding, Thermogroup Ltd T/A ThermoSphere, Bridge House, Hop Pocket Lane, Paddock Wood, TN12 6DQ.

the Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- a) The name and details of the Company, its data protection officer, and any applicable third party data controllers;
- b) The purposes for which the Company processes personal data;
- c) Details of the categories of personal data collected, held, and processed by the Company; and the categories of data subject to which that personal data relates;
- d) Details (and categories) of any third parties that will receive personal data from the Company;
- e) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- f) Details of how long personal data will be retained by the Company; and
- g) Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

A.10.1. Data Subject Access

- a) A data subject may make a **subject access request ("SAR") at any time** to find out more about the personal data which the Company holds about them. The Company is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests and in such cases the data subject shall be informed of the need for the extension).
- b) All subject access requests received must be forwarded to the DPO.

The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive

A.10.2. Redress

a. Rectification of Personal Data

- a) If a data subject informs the Company that personal data held by the Company is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of **receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension)**.
- c) In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

b. Erasure of Personal Data

- d) Data subjects may request that the Company erases the personal data it holds about them in the following circumstances:
 - b) It is no longer necessary for the Company to hold that personal data with respect to the purpose for which it was originally collected or processed;
 - p) The data subject wishes to withdraw their consent to the Company holding and processing their personal data;
 - q) The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part A.3.2 of this Policy for **further details concerning data subjects' rights to object**);
 - r) The personal data has been processed unlawfully;
 - s) The personal data needs to be erased in order for the Company to comply with a particular legal obligation.
- g) Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and

the data subject informed of the erasure, within one month of **receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension)**.

- e) In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

a) The Company shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken immediately to amend or erase that data, as appropriate.

A.11.2. Privacy Impact Assessment

A. The Company shall carry out Privacy Impact Assessments when and as **required under the Regulation. The Company's data protection officer shall** oversee privacy Impact Assessments to address the following areas of importance:

- a) The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;
- f) Details of the legitimate interests being pursued by the Company;
- g) An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- h) An assessment of the risks posed to individual data subjects; and
- i) Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

A.12 Information security

A.13.2. Transferring Personal Data to a Country outside the EEA

- a) **The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.**
- j) The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:
- c) The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

- t) The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved **by a supervisory authority (e.g. the Information Commissioner's Office)**; certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
- u) The transfer is made with the informed consent of the relevant data subject(s);
- v) The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);
- w) The transfer is necessary for important public interest reasons;
- x) The transfer is necessary for the conduct of legal claims;
- y) The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
- z) The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.