

1. Introduction

This Policy sets out the obligations of TBF Thompson (Garvagh) Ltd incorporating TBF Thompson DAF Trucks and TBF Construction Machinery (“the Company”) regarding data protection and the rights of customers, suppliers, and employees (“data subjects”) in respect of their personal data under the General Data Protection Regulation (“the Regulation”).

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. Please read this Privacy Policy as it includes important information regarding your personal data and other information.

Our websites may include links to other websites including those of our manufacturers which are not covered by this privacy policy. We therefore encourage you to review their own Privacy Policies when visiting them as we do not accept responsibility of liability for the privacy practices of third party websites.

Data protection registration

TBF Thompson are registered as a data controller with the UK Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Our data protection registration number is Z9129904

2. The Data Protection Principles

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:

- processed lawfully, fairly, and in a transparent manner in relation to the data subject;
- collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;
- 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.

3. What type of data does the Company collect?

Personally identifiable information could include your name, address, telephone number, gender, business role, email address, job title, type of business, fleet composition and driver licence number.

In order to secure certain payments, we may also collect your credit card number and expiration date, billing address etc. In addition, we may collect financial information from you (e.g., your bank account information, VAT number) as is necessary to facilitate payments and information required for VAT purposes.

Other information we collect about you that by itself is not personally identifiable information but if combined with personally identifiable information could be used to personally identify you includes your IP address. Your "IP Address" is a number that is automatically assigned to the computer that you are using by your Internet Service Provider (ISP). Collecting IP Addresses is standard practice and is done automatically by many websites, applications and other services.

Personal information such as name, telephone number and email address is collected via our websites – e.g. when you express an interest in one of our products or services.

We may collect personal information offline at marketing events or during phone calls with sales representatives or when you place an inquiry via the telephone.

TBF Thompson uses cookies to record the preference of website visitors to our commercial vehicle websites:

- www.tbftompsondaf.com
- www.tbftompsondafgarvagh.com
- www.tbftompsondafportadown.com

Cookies are small text files that are placed on your computer by websites that you visit. You can find out more information about how we use Cookies in our Cookie Statement at the bottom of the above websites. TBF Thompson do not use cookies on our corporate website, www.tbftompson.com

Additionally, HR records could include personally identifiable information such as date and place of birth, gender, national insurance number, disabilities, unspent criminal offences, past employment data, details of community association and next of kin specifics.

CCTV surveillance cameras are in operation in all depots for the purposes of crime prevention and public and employee safety. Clear and prominent signs are in place at the entrance to the buildings and in other prominent locations. These signs display the organization responsible for the signage and who to contact with any queries. TBF Thompson recognize that CCTV images are considered as personal data and as such CCTV footage is retained for no longer than is necessary in line with our Data Protection and Data Retention Policy.

Images are stored safely and securely where only a limited number of authorized TBF Thompson personnel and G4S Security staff have access to them.

If you submit to us any personally identifiable information in relation to another individual, you therefore represent that you have the authority to do so and permit us to use the information in accordance with this policy.

4. Why do we need your personal data?

The Company requires personally identifiable information to:

- respond to your web inquiries.
- contact you regarding your purchase.
- consider and respond to your job application.
- send you information and updates related to your purchase – e.g. invoices, statements, email notifications or other information that you have specifically requested.
- Where it is in accordance with your marketing preferences or if you are already trading with us as a customer, we may send email marketing communications to you regarding products or services which we think may be of interest. You have an option to unsubscribe or opt out of TBF Thompson marketing communications, product or service information.
- In an ongoing effort to understand and serve our customers better, we occasionally conduct customer satisfaction surveys and research on our customer demographics, interests and buying pattern based on personal data and other information that we have collected. This research is typically conducted on an aggregate basis only that does not identify you. Once personal data is in an aggregated form, for purposes of this Privacy Policy, it becomes non-personal data.
- HR records are maintained within the Company to comply with our responsibilities under UK law, under Fair Employment legislation and to meet the needs of our

Equal Opportunities policies. Details such as next of kin are kept on file to protect employees and for health and safety reasons. All employees involved in recruitment and selection are aware that data protection rules apply and will handle your information with respect.

- The Company uses IP Addresses to calculate usage levels of its websites and monitor the regions from which you navigate to TBF Thompson's sites.

The Company will only collect and process personal data where at least one of the following applies:

- I. the data subject has given consent to the processing of his or her personal data;
- II. processing is necessary for the performance of a contract to which the data subject is a party e.g. processing credit card details in order to affect payment or in order to take steps at the request of the data subject prior to entering into a contract;
- III. the data is required for legitimate business interests. These include but are not limited to opening a credit account to make a credit purchase and monitoring staff access to systems and downloads;
- IV. processing is necessary for compliance with a legal obligation to which the controller is subject e.g. reporting of statistics to government bodies;

Except as provided in this policy, we will not provide your personal information to third parties.

5. The Rights of Data Subjects

The Regulation sets out the following rights applicable to data subjects:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure (also known as the 'right to be forgotten');
- The right to restrict processing;
- The right to data portability;
- The right to object;

6. Accuracy of Data and Freedom of Choice

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 periodically thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken to amend or erase that data, as appropriate. If you wish to tell us of changes to

your personal details or to correct details we hold about you, you should email the Company with your request to dpo@tbftompson.com

7. Secure Processing and Data protection

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

- All emails containing personal data must be encrypted using GDPR compliant mail servers;
- 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 on site, and electronic copies should be deleted securely;
- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- All personal data stored electronically should be backed up daily with backups stored onsite **and** offsite;
- All electronic copies of personal data should be stored securely using passwords and data encryption;
- 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;
- 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.

In addition to the measures above, when working with sensitive personal data the following added security measures and protection is applied:

- Sensitive 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.

- Where sensitive 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;
- All hardcopies of sensitive personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;
- Sensitive personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, or other parties at any time;
- If sensitive 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 screen (by pressing the Window key followed by L) before leaving the device;

8. International Transfers of Data

We are committed to the security of your personal data and will not transfer data outside of the EU unless adequate safeguards are in place to ensure that your rights are protected.

We use Mailchimp to hold customer distribution lists and to create and send marketing email campaigns i.e. Mailchimp are a data processor for TBF Thompson. Since Mailchimp data is located in the U.S., we are performing a cross-border data transfer to the US.

The GDPR states that personal data shall not be transferred to a country or territory outside the EEA 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 data. One legal ground for transferring personal data is an “adequacy decision” and TBF Thompson believe that an adequate level of protection exists in the organization and country to where it is being transferred. We invite you to check out Mailchimp’s own privacy policy at <https://mailchimp.com/legal/privacy/>

In addition, Mailchimp are subject to the regulatory enforcement powers of the U.S. Federal Trade Commission and have a data privacy shield*

*The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States.

9. Data Erasure and the Right “to be forgotten”

The Company shall not keep personal data for any longer than is necessary considering the purposes for which that data was originally collected and processed. Notwithstanding we are required under UK tax law to keep your basic personal data (e.g. name, address, contact details) for a minimum of 6 years after which time it may be destroyed.

Furthermore, where the expected life of a product exceeds 6 years, customer sales invoices and relating vendor invoices are retained for longer periods to accommodate customers requiring access to their historical data after the 6-year statutory period has ended. When the data is no longer required, all reasonable steps will be taken to erase it.

The information we use for marketing purposes will be retained until you notify us that you no longer wish to receive this information. You may opt out of receiving future promotional and marketing messages from us by clicking the "Unsubscribe" link found in the footer of our emails. Please note that if you opt out of promotional and marketing messages, you may continue to receive certain communications from us, such as notifications about your account.

The Company retains HR Records as follows:

- Application Forms and Interview Notes are retained for a period of 12 months. Successful job applicant's documents are transferred to the appropriate personnel file and retained throughout the employee's period of employment.
- Personnel files and training records (including disciplinary records and working time records) are retained for 6 years after employment ceases.
- Wages and salary records (also overtime, bonuses, expenses) are retained for 6 years after employment ceases.

Employment records are kept secure and only staff with proper authorisation have access to them.

Data subjects may under certain circumstances request that the Company erases the personal data it holds about them. 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).

10. Subject Access Requests

The Company recognizes that individuals have a right to ask for access to their personal data held by TBF Thompson as well as to know if and how it is being processed. Subject Access Requests provide a right to see the information contained in personal data, rather than a right to see the documents that include that information. The company cannot refuse unless there are substantial grounds for doing so.

A policy is in place to ensure that SAR's are responded to within the legal timeframes and staff are aware of the policy and know how to respond appropriately. Once satisfied with the identity of the applicant and a clear, written request has been received, we must deal with it within one calendar month. Our response should include:

- How and to what purpose personal data is processed

- The period we intend to process it for
- Anyone who has access to the personal data
- The logic involved and legal basis used in any automatic personal data processing
- If and why we have refused to disclose information
- The subject's right to request correction of data and erasure (if we no longer process it)
- A copy of our Privacy Policy will be included

We have compiled template response letters to ensure that all elements of a response to an SAR are complied with under the GDPR regulation.

11. Privacy Impact Assessments

The Company shall carry out Privacy Impact Assessments when and as required under the Regulation. This allows the Company to evaluate processes which may impact data privacy, and take adequate steps to reduce any risks.

12. Data Breach Notification

Procedures are in place to ensure that all personal data breaches are reported immediately to the Company's DPO and that the ICO are notified within 72 hours of discovery.

In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the data protection officer will ensure that all affected data subjects are informed of the breach directly and without undue delay. Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

13. Changes to this Privacy Policy

Our business may change from time to time. As a result, at times it may be necessary for us to make changes to this Privacy Policy. We reserve the right, in our sole discretion, to update or modify this Privacy Policy at any time. Please review this Privacy Policy periodically, and especially before you provide any personal data. This Privacy Policy was

last updated on the date indicated below.

14. Contact Us

If you have any questions or concerns about this policy or wish to exercise any of your rights as a data subject you can contact us by emailing the GDPR Compliance Officer on dpo@tbfthompson.com or by mail addressed to the GDPR Compliance Officer at TBF Thompson (Garvagh) Ltd, 6-10 Killyvalley Road, Garvagh, Coleraine, BT51 5JZ

15. Implementation of Policy

This policy shall be deemed effective as of 9th April 2018 and is compliant with the GDPR which came into force on 25 May 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:	John Deighan
Position:	Financial Director
Date	24.05.24
Next review due	24.05.26
Signature:	

