TFS TRANS-BRIDGE FREIGHT SERVICES LTD

Data Protection Policy

Trans Bridge Freight is a data processor and controller under the GDPR.

Senior management and all those in managerial or supervisory roles throughout Trans Bridge Freight are responsible for developing and encouraging good information handling practices within the company. Responsibilities are set out in individual job descriptions.

The GDPR Compliance Officer should be a member of the senior management team. They are responsible to Trans Bridge Freight's Board of Directors for the management of personal data within the company, and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

- development and implementation of the GDPR as required by this policy; and
- security and risk management in relation to compliance with the policy.

The GDPR Compliance Officer, who the Board of Directors considers to be suitably qualified and experienced, has been appointed to take responsibility for Trans Bridge Freight's compliance with this policy on a day-to-day basis. In particular, they have direct responsibility for ensuring that the company complies with the GDPR, as do managers in respect of data processing that takes place within their area of responsibility.

The GDPR Compliance Officer has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for Employees / Staff seeking clarification on any aspect of data protection compliance.

Compliance with data protection legislation is the responsibility of all Trans Bridge Freight employees / contractors who process personal data.

Trans Bridge Freight's training policy sets out specific training and awareness requirements in relation to specific roles and Trans Bridge Freight employees and contractors more generally.

Individuals are responsible for ensuring that any personal data about them and supplied by them to Trans Bridge Freight is accurate and up-to-date.

Trans Bridge Freight's Board of Directors and management, located at 384 Heywood Old Road, Middleton, Manchester M24 4SB are committed to compliance with all relevant EU and Member State laws in respect of personal data. They are also committed to the protection of the rights and freedoms of individuals whose information Trans Bridge Freight collects and processes in accordance with the General Data Protection Regulation (GDPR).

Compliance with the GDPR is described by this policy and other relevant policies such as the company's Information Security Policy, along with connected policies, processes and procedures.

Trans Bridge Freight has established objectives for data protection and privacy, which are in the company's Management Review and the company's GDPR Compliance Strategy.

The company's GDPR Compliance Officer is responsible for reviewing the register of processing annually in the light of any changes to Trans Bridge Freight's activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the supervisory authority's request. This policy applies to all employees, contractors and interested parties of Trans Bridge Freight such as outsourced suppliers. Any breach of the GDPR will be dealt with under Trans Bridge Freight's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Partners and any third parties working with or for Trans Bridge Freight, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by Trans Bridge Freight without having first entered into a data confidentiality agreement, which imposes on the third-party obligations no less onerous than those to which Trans Bridge Freight is committed, and which gives Trans Bridge Freight the right to audit compliance with the agreement.

Data protection principles
Personal data must be processed lawfully, fairly and transparently.

Lawful
A lawful basis for processing must be identified before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

Fairly
In order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

Transparently
The GDPR has increased requirements about what information should be available to data subjects. These are detailed in Articles 12, 13, and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language. A Trans Bridge Freight's Privacy Notice Procedure has been established.

The special information must at minimum include:

- The identity and the contact details of the controller and, if any, of the controller's representative;
- The contact details of the GDPR Compliance Officer;
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- The period for which the personal data will be stored;
- The existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
- The categories of personal data concerned;
- The recipients or categories of recipients of the personal data, where applicable;
- Where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- any further information necessary to guarantee fair processing.

Data Protection Policy

Personal data can only be collected for specific, explicit and legitimate purposes. Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of Trans Bridge Freight's GDPR register of processing. The company's Privacy Procedure sets out the relevant procedures.

Personal data must be adequate, relevant and limited to what is necessary for processing (data minimisation)

- The GDPR Compliance Officer is responsible for ensuring that Trans Bridge Freight does not collect information that is not strictly necessary for the purpose for which it is obtained.
- All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be include a fair processing statement or link to privacy statement and approved by the GDPR Compliance Officer.
- The GDPR Compliance Officer will ensure that all data collection methods are reviewed (yearly) by internal audit, to ensure that collected data continues to be adequate, relevant and not excessive.

Personal data must be accurate and kept up to date with every effort to erase or rectify without delay.

- Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

- The GDPR Compliance Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

- It is data subjects' responsibility to ensure that data held by Trans Bridge Freight is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

- Trans Bridge Freight employees / contractors are required to notify the company when changes to their personal data occur, to enable personal records to be updated accordingly. This can be done via the Rectification of Inaccurate Data Procedure and associated form. It is Trans Bridge Freight's responsibility to ensure that any notification regarding change of circumstances is recorded and acted upon.

- The GDPR Compliance Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

- The GDPR Compliance Officer will on a yearly basis review the retention dates of all the personal data processed by Trans Bridge Freight, by reference to the data inventory. They will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Secure Disposal of Storage Media Procedure.

- The GDPR Compliance Officer is responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests. If Trans Bridge Freight decides not to comply with the request, the GDPR Compliance Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

- The GDPR Compliance Officer is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

- Where personal data is retained beyond the processing date, it will be [minimised / encrypted / pseudonymised] in order to protect the identity of the data subject in the event of a data breach. This is documented in the company's Data Retention Procedure.
- Personal data will be retained in line with the company's Data Retention Procedure. Once its retention date has passed, it must be securely destroyed as per the provisions of procedure.
- The GDPR Compliance Officer must specifically approve any data retention that exceeds the retention periods defined in data retention procedure. The procedure must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

Personal data must be processed in a manner that ensures the appropriate security.

- The GDPR Compliance Officer will carry out a risk assessment taking into account all the circumstances of Trans Bridge Freight's controlling or processing operations.
- In determining appropriateness, the GDPR Compliance Officer should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on Trans Bridge Freight itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical measures, the GDPR Compliance Officer will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave company premises;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to Trans Bridge Freight (for example ISO 270001).

When assessing appropriate organisational measures, the GDPR Compliance Officer will consider the following:

- The appropriate training levels throughout Trans Bridge Freight;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper-based records;
- Adoption of a clear desk policy;
- Storing of paper-based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace (or implementing a BYOD procedure);
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

Trans Bridge Freight's compliance with this principle is contained in its Information Security Management System (ISMS), which has been developed in line with ISO/IEC 27001:2013 and the company's information security policy.

The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

- The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements.
- Trans Bridge Freight will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

Data subjects' rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- To not have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the GDPR.
- To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- To request the supervisory authority to assess whether any provision of the GDPR has been contravened.
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- To object to any automated profiling that is occurring without consent

Trans Bridge Freight ensures that data subjects may exercise these rights:

- Data subjects may make data access requests as described in Subject Access Request Procedure. This procedure also describes how Trans Bridge Freight will ensure that its response to the data access request complies with the requirements of the GDPR.
- Data subjects have the right to complain to Trans Bridge Freight regards the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure.

Consent

- Trans Bridge Freight understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.
- There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation, usually via the company's privacy notice.
- For sensitive data, explicit written consent must be obtained unless an alternative legitimate basis for processing exists. The company's Consent and Consent Withdrawal Procedure address this.
- In most instances, consent to process personal and sensitive data is obtained routinely by Trans Bridge Freight using standard consent documents, for example when a new client signs a contract, or during induction for participants on programmes.
- Trans Bridge Freight does not provide online services to children.
- Consent must be separate from other terms and conditions and should not be a precondition of signing up to that service unless necessary for that service.
- The company's privacy notice explains why Trans Bridge Freight will rarely use consent as a lawful basis for processing due to the often-unbalanced relationship between Trans Bridge Freight and the data subject.

Security of data

All Trans Bridge Freight employees / contractors are responsible for ensuring that any personal data held by the company, and any data for which they are responsible, is kept securely. It is not to be disclosed to any third party unless that third party has been specifically authorised by Trans Bridge Freight to receive that information and has entered into a confidentiality agreement. The company has standard NDA's.

All personal data should be accessible only to those who need to use it. The company has strict physical security controls (as laid out in the company's Physical Security Procedure). Access to personal data may only be granted in line with the Access Control Policy.

All personal data should be treated with the highest security and must be kept:

- In a lockable room with controlled access; and/or
- In a locked drawer or filing cabinet; and/or
- If computerised, password protected in line with corporate requirements in the Access Control Policy; and / or
- Stored on (removable) computer media which are encrypted in line with the company's procedure concerning secure disposal of storage media.

Care must be taken to ensure that PC screens and terminals are not visible except to authorised Trans Bridge Freight employees/contractors. All individuals are required to enter into an Individual User Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with the company's retention procedure

Personal data may only be deleted or disposed of in line with the company's retention procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as per the company's procedure governing the secure disposal of storage media.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site. The company has dedicated procedures addressing working from home, flexible working, remote working, etc.

Disclosure of data

Trans Bridge Freight must ensure that personal data is not disclosed to unauthorised third parties. This includes family members, friends, government bodies, and in certain circumstances, the police. Certain circumstances may necessitate disclosure to interested third parties (for example complying with a legal or regulatory obligation, to safeguard national security, to protect the data subject's vital interests, in the discharge of regulatory functions or in the detection and prevention of a crime).

All employees/contractors should exercise caution when asked to disclose personal data held on another individual to a third party and may be required to attend specific training that enables them to deal effectively with any such risk. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Trans Bridge Freight's business.

All requests to provide data for one of these reasons must be supported by appropriate paperwork. All such disclosures must be specifically authorised by the GDPR Compliance Officer. They will be treated as special-circumstance subject access requests and addressed in the company's subject access request procedure.

Retention and disposal of data

Trans Bridge Freight shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

Trans Bridge Freight may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data is set out in the company's retention of records procedure, along with the criteria used to determine this period including any statutory obligations Trans Bridge Freight has to retain the data.

Trans Bridge Freight's data retention and data disposal procedures will apply in all cases.

Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure.

Data Transfers

All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate level of protection for the fundamental rights of the data subjects.

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

An adequacy decision

- The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances, no authorisation is required. Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision. A list of countries that currently satisfy the adequacy requirements of the Commission are published in the Official Journal of the European Union. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Privacy Shield

- If Trans Bridge Freight wishes to transfer personal data from the EU to an organisation in the United States it should check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

Assessment of adequacy by the data controller. In making an assessment of adequacy, the UK based exporting controller should take account of the following factors:

- The nature of the information being transferred;
- The country or territory of the origin, and final destination, of the information;
- How the information will be used and for how long;
- The laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- The security measures that are to be taken as regards the data in the overseas location.

Binding corporate rules

Trans Bridge Freight may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that the company is seeking to rely upon.

Model contract clauses

Trans Bridge Freight may adopt approved model contract clauses for the transfer of data outside of the EEA. If Trans Bridge Freight adopts the model contract clauses approved by the relevant supervisory authority, there is an automatic recognition of adequacy.

Exceptions

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- The transfer is necessary for important reasons of public interest;
- The transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

Information asset register/data inventory

Trans Bridge Freight has established a data inventory as part of its approach to address risks and opportunities throughout its GDPR compliance project. The inventory addresses:

- Business processes that use personal data;
- Source of personal data;
- Volume of data subjects;
- Description of each item of personal data;
- Processing activity;
- Maintains the inventory of data categories of personal data processed;
- Documents the purpose(s) for which each category of personal data is used;
- Recipients, and potential recipients, of the personal data;
- The role of Trans Bridge Freight throughout the data flow;
- Key systems and repositories;
- Any data transfers
- All retention and disposal requirements

Trans Bridge Freight is aware of any risks associated with the processing of particular types of personal data.

- Trans Bridge Freight assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) are carried out in relation to the processing of personal data by Trans Bridge Freight, and in relation to processing undertaken by other organisations on behalf of Trans Bridge Freight.
- Trans Bridge Freight shall manage any risks identified by the risk assessment in order to reduce the likelihood of a nonconformance with this policy.
- Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Trans Bridge Freight shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.
- Where, as a result of a DPIA it is clear that Trans Bridge Freight is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not Trans Bridge Freight may proceed must be escalated for review to the GDPR Compliance Officer.
- The GDPR Compliance Officer shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.
- Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to Trans Bridge Freight's documented risk acceptance criteria and the requirements of the GDPR.

Records

This document is categorised as private and should not be shared outside the company unless it is part of a binding corporate contract.

All documentation relating to personal data are bound by the articles laid down by the GDPR. Trans Bridge Freight takes appropriate technical and organisational measures to ensure that the rights of the data subject, and the responsibilities of the data controller and processor, are maintained and enforced.

Personal data is processed in line with the Trans Bridge Freight Data Processing Matrix and the company's Data Retention and Destruction Matrix and Data Retention and Destruction Procedure

Review

This document will be reviewed yearly, or unless a material change in UK law necessitates a change in the way organisations categorise and process personal and sensitive data.

Trans Bridge Freight maintains records of all data transfers. These records will be retained in accordance with GDPR principles and with the company's Data Retention and Destruction Policy.