

Trojan Special Fasteners Ltd

Employee Privacy Policy

18 Fortnum Close
Tile Cross
Birmingham
B33 0LG

1 Employee Privacy Policy

As your employer, *The Company* needs to keep and process information about you for normal employment purposes necessary to manage the employment relationship. *The Company* is committed to being transparent about how it collects and uses that information and to meeting its data protection obligations. This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

1.1 What personal data do we process?

Employee information processed includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers, this may include your curriculum vitae, application forms completed;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your bank account and NI number;
- information about your marital status, next of kin, dependents and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- details of your working schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any 'active/live' warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence;
- details of any company loans, training agreements and records, or other agreements entered into with *The Company*;
- eligibility to drive, including licence details or points on licence for those employee's who drive for work;
- electronic information in relation to your use of IT systems / swipe cards / telephone systems
- your image (whether captured on CCTV, by photograph or video)
- information about medical or health conditions, including whether or not you have a disability for which *The Company* needs to make reasonable adjustments;
- any other category of personal data which *The Company* may notify you of from time-to-time

1.1.1 Collection of Personal Data

Much of the information we hold will have been provided by you. For example, on application forms, CVs, during interviews, gathered from identity documents, forms completed by you at the start of or during employment or through meetings or other assessments. In some cases, information will be gathered from other internal sources, such as your line manager.

In other cases, *The Company* may collect personal data about you from external sources, such as references from former employers. Third party data collection will only be completed with your consent.

1.1.2 Why The Company processes personal data?

A. To fulfill the employment contract

The Company needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer other benefits that may apply such as pension and insurance entitlements.

B. To comply with legal obligation

The Company needs to process some data to ensure compliance with legal obligations. For example, it is required to check an employee's entitlement to work in the State, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.

C. For other legitimate purposes

The Company has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows *The Company* to:

- run equal opportunity recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including Parenting Leave, Sickness Absences, Unpaid Leave), to allow effective workforce management, to ensure that *The Company* complies with legal duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- provide references on request for current or former employees; and
- respond to and defend against legal claims.

Some special categories of personal data, such as information about health or medical conditions, are processed to fulfill employment law obligations, particularly in relation to employees with disabilities.

1.1.3 Automated decision-making - does not occur

The Company does not rely solely on automated decision making to reach employment decisions.

1.1.4 Special Categories

Where we process special categories of information relating to your racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union memberships, or sexual orientation, we will always obtain your explicit consent to those activities unless this is not required by law or the information is required to protect your health in an emergency. Processing of such data is done for the purposes of equal opportunities monitoring.

1.1.5 Consent

Where we are processing data based on your consent, you have the right to withdraw that consent at any time.

Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

1.1.6 Computers and Email

In addition, we monitor computer, email and telephone use, as detailed in our Company Handbook.

1.2 Who has access to data?

Other than as mentioned below, we will only disclose information about you to third parties if we are legally obliged to do so.

1.2.1 Internally

Your information may be shared internally, including with members of the HR and team (including payroll), your line manager, managers in the business area in which you work and IT staff. Only data necessary for the performance of their role will be shared with individuals.

1.2.2 Third parties

The Company occasionally shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks. *The Company* may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The Company also shares your data with third parties that process data on its behalf, in connection with payroll, the provision of benefits and the provision of occupational health services.

1.2.3 BrightPay Connect

All employees will have access to the BrightPay Connect employee self-service portal. Using personal login credentials, employees will be able to view much of their personal information held by *The Company*.

1.3 Data Storage and Security

The Company takes the security of your data seriously.

HR-related personal data is held on the individual's personnel file, in hardcopy or electronic format, or both, and on any HR or IT system in use. Further details on data security measures can be found in *The Company's* Data Protection Policy.

Where *The Company* engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

1.3.1 For how long does The Company keep your data?

Where statutory retention periods exist, your personal data will be stored for the duration of these periods. *The Company* will conduct an audit on employee files once a year and remove files that have exceeded the statutory retention period at that point.

Other general employee data, which may include but is not limited to; employment contracts, performance appraisals, training records, disciplinary or dismissal records, and grievance records, will be held for the duration of employment (unless otherwise stated) and for six years after the termination of employment.

1.3.2 Data Subject Access Request

If you would like to make a subject access request in relation to your own personal data you should make this in writing to Privacy Policy v1, *The Company* must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months. In some cases, *The Company* may need to ask for proof of identification before the request can be processed.

If a subject access request is made, *The Company* will confirm:

- the purposes of any processing
- the categories of personal data concerned
- the recipients to whom the personal data has been or will be disclosed to, including recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers
- where possible, the period for which the personal data will be retained or the criteria for determining that period
- the individual's right to request rectification or erasure of personal data or restriction of processing of personal data
- the right to lodge a complaint with the Information Commissioner
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.
- the purposes of any processing

The Company will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless otherwise agreed.

There is no fee for making a subject access request. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request. Where additional copies of documentation are required a fee based on the administrative cost of providing the additional copies will be charged. A subject access request is likely to be unfounded or excessive where it repeats a request to which *The Company* has already responded. Should *The Company* receive an unfounded or excessive request they will write to the individual confirming this is the case and whether or not they are in a position to respond.

1.3.3 International Transfer: Data transferred outside the EEA for storage purposes

Ordinarily, *The Company* will not transfer your data to countries outside the European Economic Area. In some cases, personal data will be saved on storage solutions that have servers outside the European Economic Area (EEA), [for example, Dropbox or Google]. Only those storage solutions that provide secure services with adequate relevant safeguards will be employed

1.4 Your rights

- run equal opportunity recruitment and promotion processes;
- access and obtain a copy of your data on request primarily by way of a subject access request (see above);
- require *The Company* to change incorrect or incomplete data;
- require *The Company* to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where *The Company* is relying on its legitimate interests as the legal ground for processing.
- Request that *The Company* erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected.
- request human intervention where automated decision making exists.

If you believe that *The Company* has not observed your data protection rights, you can contact the Information Commissioner.

1.4.1 What if you do not provide personal data?

Under your contract of employment, you are obliged to provide *The Company* with certain data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide *The Company* with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable *The Company* to enter a contract of employment with you. If you do not provide other information, this will hinder *The Company's* ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

1.4.2 Data Controller Details

Trojan Special Fasteners Ltd, 18 Fortnum Close, Tile Cross, Birmingham, is the data controller of data for the purposes of the GDPR.

If you have any concerns as to how your data is processed, or if you wish to exercise any of your rights outlined above, you can contact:

- Privacy Policy v1- Mobeen Ali.