THERMIT WELDING (GB) LIMITED
Data Protection Policy
for Employees, Workers, Apprentices and Consultants

Data Protection Policy
for Employees, Workers and Consultants

1. Introduction

The Company takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our employment relationship with you. We will comply with our legal obligations under the Data Protection Act 2018 and the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security.

The Company has measures in place to protect the security of your data. This includes, but is not limited to, a Data Security Policy

The Company is a '**data controller**' for the purposes of your personal data. This means that the Company determines the purpose and way we process your personal data. The Company will only hold data for as long as necessary for the purposes for which we collected it. In this context, the Company may include a person nominated within each Company Department.
This Policy explains how the Company will hold and process your information and/or data. It explains your rights under the current Data Protection Act and GDPR legislation. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Company.

This Policy does not form part of your Contract of Employment (or Contract for Services, if relevant) and can be amended by the Company at any time. It is intended that this Policy is fully compliant with the Data Protection Act and the GDPR.

2. Scope

This Policy applies to current and former Employees, Workers, Apprentices and Consultants. If you fall into one of these categories, then you are a '**data subject**' for the purposes of this Policy. You should read this Policy alongside your Contract of Employment (or Contract for Services) and any other notice we issue to you from time to time in relation to your data.

This Policy applies to all personal data, whether it is stored electronically or on paper.

3. Data Protection Principles

Personal data must be processed in accordance with 6 '**Data Protection Principles**.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;

- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

4. Personal Data

For the purposes of this Policy, '**Personal data**' means information which relates to a living person who can be identified from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This personal data might be provided to us by you, or someone else (such as a former employer, your doctor etc.), or it could be created by us. It could be provided or created during the recruitment process or during the course of the Contract of Employment (or services) or after its termination. It could be created by your Line Manager or other colleagues.

We will collect and use the following types of personal data about you:

- Details of your bank account(s) and National Insurance (NI) number and other pay-related information;

Your name, date of birth, address, telephone numbers, your next-of-kin/emergency contact details;
Application Forms (which will include details of your employment history, qualifications, skills and experience);
Copies of Passports and other identity/nationality related information (to ensure you have the legal right to work in the UK);
Contracts of Employment (which includes such information as your pay and benefits);
Information about endorsements on Driving Licences;
Health Questionnaires and other information about your health and sickness records (for health surveillance, investigations into health issues and concerns, first aid and health and safety purposes – see special categories of data below);
Obtaining occupational health and medical advice, to ensure that the Company complies with its duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensures that employees are receiving the pay or other benefits to which they are entitled;
Information relating to family leave and sabbaticals;
Information related to any investigations as part of the Company's Disciplinary or Grievance Procedures, including warnings, statements and other related correspondence;
Assessments of your performance (informal and formal), training you have participated in, performance related PIP's (Performance Improvement Plans);
Information about your age, sex, ethnic origin and disability in order to ensure compliance with the Company's Equal Opportunities Policy and to enable the Company to make any reasonable adjustments required; and
any other category of personal data which we may notify you of, from time to time.

5. **Special categories of personal data**

'**Special categories of personal data**' are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health;
- your sexual orientation; and
- CCTV footage.

We may hold and use any of these special categories of your personal data in accordance with the law.

6. **Processing**

'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making data available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system.

The Company will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act. You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights below.

We can process your personal data for these purposes without your separate knowledge or consent at the time, as long as this is necessary as part of our business and/or to manage our employment relationship with you. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data, you should be aware that we may not be able to carry out certain parts of the Contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have, such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may have.

We will only process special categories of your personal data (see above) in certain situations in accordance with the law; for example, we can request a medical report if we have your explicit consent. If we asked for your consent to process a special category of personal data, then we would explain the reasons for our request. You do not need to give consent and can withdraw consent later if you choose by contacting Human Resources. We do not need your explicit consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law;

- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of the assessment of your working capacity.

We might process special categories of your personal data for the purposes outlined above which have an asterisk beside them. In particular, we may use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities; and
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety.

We do not make automated decisions about you, using your personal data, or use profiling in relation to you.

7. Sharing your personal data

Sometimes we might share your personal data with other companies to which we are associated, or our contractors and agents to carry out our obligations under our Contract with you or for our legitimate interests, for example our HR Consultants, I.T. Consultants, Pension Providers etc.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

8. Employees processing personal data for the Company

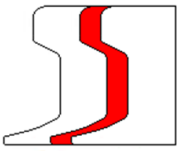
Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's Data Security and Data Retention policies.

Human Resources are responsible for reviewing this Policy and updating the Board of Directors on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this Policy or data protection to this department.

You should only access personal data covered by this Policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

You should not share personal data informally. You should keep personal data secure and not share it with unauthorised people. You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.



You should use strong passwords e.g. with a combination of letters, numbers etc. and this should be changed regularly. You should always ensure that you lock your computer screen prior to moving away from your desk. You should also ensure that your automatic setting is switched on in the event that you forget to lock your screen; this should be set to come on at 1 minute after your screen has been left idle.

Personal data should be encrypted before being transferred electronically to authorised external contacts. You should consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

Do not save personal data to your own personal computers or other devices. You should lock drawers and filing cabinets when you are away from your desk/office if they contain personal data. You should not leave paper containing personal data unattended.

You should not take personal data away from Company's premises without authorisation from your Line Manager. Personal data should be shredded and disposed of securely when you have finished with it.

You should ask for help from Human Resources if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

Any deliberate or negligent breach of this Policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure. It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

9. Data breaches

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must keep evidence of that breach.

If a breach is likely to result in a risk to the rights and freedoms of individuals, then we will also notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact your Line Manager and Human Resources immediately, and keep any evidence you have in relation to the breach.

10. Subject access requests

Data subjects can make a '**subject access request**' ('SAR') to find out what information we hold about them. This request must be made in writing. If you receive such a request, you should forward it immediately to Human Resources who will coordinate a response.

If you would like to make a SAR in relation to your own personal data, you should make this in writing to Human Resources. We must respond within 1 month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further 2 months.

There is no fee for making a SAR. However, if your request is considered by the Company to be manifestly unfounded or excessive, we may charge a reasonable administrative fee or refuse to respond to your request.

11. Data subject rights

You have the right to information about what personal data we process, how and on what basis as set out in this Policy. You have the right to access your own personal data by way of a subject access request (see above).

You can request that any inaccuracies in your personal data are corrected. To do so, you should contact Human Resources. You also have the right to request that we 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. To do so you should contact Human Resources.

The Company does not necessarily have to comply with a request by deleting the data in its entirety. Depending on the reasons and legal bases for processing the data, the Company may be required to erase some categories while it may have grounds for retaining others. For example, the Company has a duty to retain records relating to payment of SSP (Statutory Sick Pay) and SMP (Statutory Maternity Pay) for at least 3 years following the end of the tax year in which they made the payment. Another example is where the request is to delete data relating to disciplinary proceedings; the Company could refuse the request on the ground that the data would be required should the employee bring a Tribunal claim relating to the disciplinary issue.

While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact Human Resources.

You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

You have the right to be notified of a data security breach concerning your personal data.

In most situations we will rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact Human Resources.

You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.