



Data Protection & Security Policy

TFI Concepts Limited takes the security and privacy of all personal data in its possession seriously, whether this belongs to employees, workers, job applicants, clients, customers or suppliers. In the course of our business, we need to gather and use information or 'data' to enable us to manage such relationships, or for legal requirements. We fully intend to comply with our legal obligation under the **Data Protection Bill** and the **EU General Data Protection Regulation** ('GDPR') and any other similar data protection legislation in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

The policy applies to current and former employees, workers, volunteers, 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 and any other notice that we may issue you with from time to time in relation to your data.

This policy explains how TFI Concepts Limited will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, TFI Concepts Limited. If you are in any doubt about what data you can or cannot disclose, you should seek advice from your line manager, or the HR department.

TFI Concepts Limited is a '**data controller**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

TFI Concepts Limited has measures in place to protect the security of your data in accordance with this policy, and will hold data in accordance with our Employee Records policy, copies of which can be obtained from the HR department. We will hold data for as long as necessary for the purposes for which we collected it, or if there is a legal basis for holding it longer.

This policy does not form part of your Contract of Employment, and can be amended by TFI Concepts Limited at any time. It is intended that this policy is fully compliant with the Bill and the GDPR however if any conflict arises between those laws and this policy, TFI Concepts Limited intends to comply with the Bill and the GDPR.

Data Protection Principles

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

- processed fairly, lawfully and transparently;
- collected and processed only for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- adequate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not to be kept for longer than is necessary for the purposes for which it is processed or necessary; and
- be processed securely.

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



Definition of Personal Data

'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 policy applies to all personal data whether it is stored electronically, on paper or on other materials. Data will be stored in a range of different places, including an employee's personnel file, in HR management systems and on other IT systems (including our email system).

This personal data might be provided to us by you, by someone else (such as a former employer, your doctor, or the Disclosure and Barring Service), or it could be created by us. It could be provided or created during the recruitment process, or during the course of your working relationship with TFI Concepts Limited, or after its termination. It could be created by your line manager or other colleagues.

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

- your name, address and contact details, including email address and telephone number, date of birth, gender and car registration number;
- information relating to the terms and conditions of your employment;
- information collected during the recruitment process, including CV/application form, references from previous employers, interview notes, copies of certificates or membership of professional bodies and any pre-employment assessments;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with us, including training records;
- information about your remuneration, including entitlement to benefits such as pensions, healthcare, death in service or other benefits;
- details of your bank account, information relating to tax status, tax code and national Insurance number;
- information about your marital status, next of kin, dependents and emergency contacts;
- information about your nationality, immigration status and entitlement to work in the UK;
- images, including CCTV images, photographs and videos, or photographic ID;
- information relating to your ability to drive (where relevant);
- information regarding your use of our IT systems, including usage of telephones, email and the internet;
- data relating to movement whilst in Company vehicles;
- details of your schedule (days of works and working hours) and attendance at work, including clocking in records;
- details of periods of leave taken by you, including the type and reasons for the leave, and any related correspondence;
- details of any disciplinary or grievance procedures, or investigations in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence;
- any termination of employment or engagement documents, including resignation letters, dismissal letters redundancy letters, minutes of meetings, settlement agreements and any related correspondence; and
- any other category of personal data which we may notify you of from time to time.

TFI Concepts Limited may also collect, process and store the following special categories of your personal data:

- information about medical or health conditions, including name and address of GP, sickness absence records, GP/Occupational Health reports and whether or not you have a disability for which we need to make reasonable adjustments;



- information about your criminal record; and
- information about your racial or ethnic origin.

Definition of Special Categories of Personal Data

'special categories of personal data' are types of personal data consisting of information including:

- your racial or ethnic origin;
- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health;
- your sex life and sexual orientation; and
- any criminal convictions and offences.

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

Definition of 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 available;
- alignment or combination; and
- restriction, destruction or erasure.

This included processing personal data which forms part of a filing system and any automated processing.

How will we process your Personal Data?

TFI Concepts Limited will process your personal data (including special categories of personal data) in accordance with our obligations under the Bill and GDPR.

We need to process data to enter into an employment contract with you and to meet our obligations under your employment contract. For example, we need to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefits, such as a pension.

In some cases, we need to process data to ensure that we are complying with our legal obligations. For example, we are required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.

In other cases, we have a legitimate interest in processing personal data before, during and after the end of the employment relationship, providing that your interests or your fundamental rights do not override our interests.



We can process your personal data for these purposes without your knowledge or consent. 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 of Employment 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 suffer from.

Examples of when we might process your personal data

We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement). For example:

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with us;
- to check you have the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance*;
- to decide whether to promote you
- to decide whether and how to manage your performance, absence or conduct*;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability*;
- to monitor diversity and equal opportunities*;
- to monitor and protect the security (including network security) of the Company, of you, our other employees, customers and others;
- to monitor and protect the health and safety of you, and other employees, customers and third parties*;
- to pay you and provide pension and other benefits in accordance with the Contract between us*;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- monitoring compliance by you, us and others with our policies and our contractual obligations*;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us*;
- to answer questions from insurers in respect of any insurance policies which relate to you*;
- running our business and planning for the future;
- the prevention and detection of fraud or other criminal offences;
- to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*; and
- for any other reason which we may notify you of from time to time.

We might process special categories of your personal data for the purposes 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;
- your sickness absence, health and medical condition to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including making reasonable adjustments and looking after your health and safety; and
- your criminal convictions, and deciding whether they pose a risk to other employees, customers and third parties.



We will only process special categories of your personal data in certain situations. Such as information about health or medical conditions or information about criminal convictions, in accordance with the law. We may also process these special categories of personal data where we have your explicit written consent, in which case, we will provide you with full details of the information that we would like and the reason for our request, so that you can consider whether you wish to consent or not.

We do not need your consent to process special categories of your personal data when we are processing it for the following purpose, which we may do:

- where it is necessary for carrying out rights/obligations under employment laws;
- where it is necessary to protect your vital interest 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 occupational medicine or for the assessment of your working capacity.

The only automated decision making that we may use is during recruitment, where we may undergo psychometric testing. If this applies to you, you will be advised and your rights explained to you.

Sharing your personal data

Your information may be shared internally, including with members of the recruitment team, your line manager, managers in the business area in which you work and IT staff if access to the data is necessary for performance of their roles.

TFI Concepts Limited also share your data with third parties, including third parties who process data on our behalf, such as previous employers (in order to obtain pre-employment references), payroll providers, benefits providers and/or administration, pension scheme providers and/or administration, occupational health providers, external auditors and organisations providing criminal record checks. We may also share your data with third parties that provide professional services such as specialist employment law guidance, or where it is necessary to administer the contract that we have entered into with you or where we need to comply with a legal obligation (e.g. detection and prevention of crime). 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.

We may also share your data with third parties in the context of a sale of some or all of our business, or in a TUPE situation. In those circumstances, the data will be subject to confidentiality arrangements.

We may also need to share your data with a regulator, or to otherwise comply with the law.

We will not transfer your personal data outside the European Economic Area unless there are adequate measures in place that ensure a level of protection equivalent to that afforded by the Bill and GDPR.

How should you process personal data for TFI Concepts Limited?

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



TFI Concepts Limited Director is responsible for reviewing this policy and the Quality & Regulatory Affairs (Q&RA) department are responsible for updating the Board of Directors on TFI Concepts Limited'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 them, or ask them if you need help or assistance. You should also inform them should you notice any areas of data protection or security that we can improve upon.

You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of TFI Concepts Limited 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 and you should keep it secure and not share it informally or with unauthorised people, and dispose of it securely when it is no longer required.

You should ensure that you use strong passwords for any computer or other device, lock your screen when away from your desk and lock any drawers and filing cabinets when not in use.

Do not leave personal data lying about and do not save any personal data to your own personal computer or any other personal device, or remove it from TFI Concepts Limited's premises without the authorisation of your line manager or the IT department.

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.

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.

How to deal with data breaches

We have robust measures in place to minimise and prevent data breaches from taking place, and have a data breach policy in place which will be followed should a breach of personal data occur (whether in respect of you or someone else).

If you are aware of a data breach, you should report it to the Director's department within 4 hours of discovering the breach using the 'Notification of Personal Data Breach' form appended to the Data Protection Breaches policy. Once completed, this form should be emailed to info@tficonceptsltd.co.uk and the Director will then investigate the breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then the Director's must also notify the Information Commissioners Office within 72 hours. Please refer to our Data Protection Breaches policy for further details.

Data security

TFI Concepts Limited takes the security of your data seriously. We have internal policies and controls in place to ensure that your personal data is not lost, accidentally destroyed, misused or disclosed, and is limited to our employees or other third parties who have a need to know for the proper performance of their duties. We will use our data breach policy to deal with any suspected data security breach, and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.



Where we engage third parties to process personal data on our behalf, they do so on the basis of written instructions, and under a duty of confidentiality and are obliged to implement appropriate technical and organisation measures to ensure the security of data.

Your data subject rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request via a subject access request;
- require the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing;
- restrict the processing of your data should you wish to establish the accuracy of the data or the reasons for processing, and
- request for the transfer of your data to another party,

If you would like to exercise any of these rights, please email info@tficonceptsltd.co.uk who will deal with your request. Alternatively, you can write to Data Protection, The Royal Arsenal Unit 30, iO Centre, Armstrong Road, London SE18 6RS.

If you believe that TFI Concepts Limited has not complied with your data protection rights, you can complain to the Information Commissioners Office (ICO), the UK supervisory authority for data protection. Full contact details including a helpline number can be found on the Information Commissioners Office website (www.ico.org.uk).

In most situation we will not 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 you consent, you should contact info@tficonceptsltd.co.uk.

Subject access request

Any data subject can make 'subject access request' (SAR) to find out the information we hold about them. This request must be in writing and emailed to info@tficonceptsltd.co.uk.

If you personally receive a SAR request from a data subject, you should forward it to info@tficonceptsltd.co.uk Who will coordinate a response.

If it is unclear what information is being requesting, we may ask the data subject to complete one of our Subject Access Request Forms. We may also request further information or any evidence relating to their identity, to ensure that the correct information is provided to the correct individual.

In all cases of SARs, we 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.



TFI CONCEPTS LIMITED

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

Signed Mike Bamber - Director

Dated 03.03.2025

TFI CONCEPTS LIMITED