# Overview & Introduction

All organisations that process *personal data* are required to comply with data protection legislation. This includes in particular the Data Protection Act and the EU General Data Protection Regulation (together the 'Data Protection Laws'). The Data Protection Laws give individuals (known as 'data subjects') certain rights over their personal data whilst imposing certain obligations on the organisations that process their data.

Employers and recruitment businesses collect and process the personal data of data subjects and so are defined as data controllers.

Data controllers need to produce appropriate documentation to demonstrate compliance with the GDPR regulations. Under Article 24 of the regulations this shall include the implementation of appropriate data protection policies. This policy provides a template for members to adapt to their own business arrangements to set out how their Company implements the Data Protection Laws.

The following terms and their meanings are included in the policy:

**'*consent*'** means any freely given, specific, informed and unambiguous indication of an individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the *processing* of personal data relating to him or her;

**'*data controller*'** means an individual or organisation which, alone or jointly with others, determines the purposes and means of the *processing* of *personal data*;

**'*data processor*'** means an individual or organisation which processes *personal data* on behalf of the *data controller*;

**'*personal data*'** means any information relating to an individual who from it can be identified directly or indirectly including through a combination of data, such as by a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

**'*personal data breach*'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, *personal data*;

**'*processing*'** means any operation or set of operations performed on *personal data*, such as collection, recording, organisation, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**'*sensitive personal data*'** means *personal data* revealing racial or ethnic origin, political opinions, religious or similar beliefs, or trade union membership, and the *processing* of genetic data, biometric data, data concerning health, an individual's sex life or sexual orientation and an individual's criminal convictions.

# Data Protection Policy

## Introduction

*Turner Stubbs Limited* 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 relationship with you. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **EU General Data Protection Regulation** ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

This policy applies to data processed regarding current and former employees and workers, job applicants, agency work seekers, agency workers and individual client contacts. 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, contract for services or client terms of business and any other notice we issue to you from time to time in relation to your data.

The Company has registered with the ICO and its registration number is Z7489544.

The Company has measures in place to protect the security of your data in accordance with our Data Security Policy. A copy of this can be obtained from Company Directors (Data Protection), 40 George Street, Nottingham, NG1 3BG.

The company will hold data in accordance with our Data Retention Policy. A copy of this can be obtained from Company Directors (Data Protection), 40 George Street, Nottingham, NG1 3BG. We will only hold data for as long as necessary for the purposes for which we collected it.

The Company 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.

This policy explains how the Company 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, the Company.

The Company will only process personal data where it has a legal basis for doing so.

The Company's Privacy Notice is available on our website.

The Company will review the personal data it holds on a regular basis to ensure it is being lawfully processed and it is accurate, relevant and up to date.

Before transferring information to a third party (e.g. past, current or prospective employers, suppliers, clients, intermediaries or any other third party), the Company will establish that it has a legal basis for making the transfer.

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 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the Company intends to comply with the 2018 Act and the GDPR.

## Data Protection Principles

Personal data must be processed in accordance with our '**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;
- be processed in accordance with the rights of data subjects;
- not be transferred to another country without appropriate safeguards being in place; and
- be processed securely.

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

## How we define 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.

This personal data might be provided to us by you, or someone else (such as a former employer, or your doctor), 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 contract for services or after its termination. It could be created by your manager or other colleagues.

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

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- your contact details and date of birth;
- the contact details for your emergency contacts;
- your gender, marital status and family details
- information about your contract of employment or contract for services including start and end dates of employment, role and location, working hours, details of promotion, salary/rates of pay (including details of previous remuneration), pension, benefits and holiday entitlement;
- your bank details and information in relation to your tax status including your national insurance number;
- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us;
- information relating to disciplinary or grievance/worker complaints and disputes investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
- information relating to your performance and behaviour at work;
- training records;
- electronic information in relation to your use of IT systems/swipe cards/telephone systems;
- your images (whether captured on CCTV, by photograph or video);
- any other category of personal data which we may notify you of from time to time.

## How we define 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 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.

## How we define 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 includes processing personal data which forms part of a filing system and any automated processing.

## How will we process your personal data?

The Company will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

We will use your personal data for:

- Compliance with a legal obligation (e.g. real time information reporting to HMRC)
- The performance of the contract (e.g. processing payroll, monitoring attendance)
- Protecting the legitimate interest of the Company or third party (e.g. collecting information during a disciplinary, grievance, complaints or disputes process, or collecting workplace data in order to improve workplace performance). You have the right to challenge our legitimate interests and request that we stop this processing. See the section on subject data access rights for further detail.

We can process your personal data for these purposes without specifically informing you or obtaining your 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 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.

## Privacy by design and default

We are required to demonstrate that privacy considerations are embedded into all our processes and procedures. We complete documented data protection impact assessments on our processes and procedures to ensure we are compliant with the principles of GDPR. This is completed each time a policy or procedure is changed.

The types of measures that we have implemented includes:

- Data minimisation (i.e. not keeping the data longer than is necessary)
- Pseudonymisation (personal data which cannot be attributed to an individual without additional information. The information must be kept separately and is subject to technical and organisational measures to ensure the individual cannot be identified)
- Anonymisation (using separate keys/codes so that individuals cannot be identified)
- Cyber security

## 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 in the UK;
- 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 complaints and disputes 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 staff, customers and others;
- to monitor and protect the health and safety of you, our other staff, 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;
- to pay trade union subscriptions;
- 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;
- for any other reason which we may notify you of from time to time.

We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so 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 consent and can withdraw consent later if you choose by contacting Company Directors (Data

Protection), 40 George Street, Nottingham, NG1 3BG We do not need your 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 occupational medicine or for the assessment of your working capacity.

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

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- 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; and
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

We do not take automated decisions about you, using your personal data or use profiling in relation to you, except where the automated/profiling decision:

- Is necessary for the entering into or performance of a contract between the Company and you;
- Is authorised by law; or
- You have given your explicit consent

## Sharing your personal data

Sometimes we might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

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.

Such activities can include payroll and any statutory or legal requirement or obligation.

We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

## How should you process 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.

The Company's board of directors are responsible for reviewing this policy and updating the Company management 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 Company Directors (Data Protection), 40 George Street, Nottingham, NG1 3BG.

The following details the key rules and good practice that apply to everyone in the Company that processes personal data and you may be subject to monitoring, inspection and risk assessment to ensure that these are being applied.

- 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 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 not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- You should use strong passwords.
- You should lock your computer screens when not at your desk.
- Personal data should be encrypted before being transferred electronically to authorised external contacts.
- 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.
- Personal data should never be transferred outside the European Union except in compliance with the law and authorisation of a Company Director.
- You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.
- You should not take personal data away from Company's premises without authorisation from your line manager or a Company Director.
- Personal data should be shredded and disposed of securely when you have finished with it.
- You should ask for help from a Company Director 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.

## How to deal with 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 take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner's Office within 72 hours.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, then we will also take appropriate steps to inform those individuals without undue delay.

If you are aware of a data breach you must contact a Company Director immediately and keep any evidence, you have in relation to the breach.

## Subject access requests

Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request, you should forward it immediately to the relevant Data Protection department (Payroll or Company Directors) 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 Company Directors (Data Protection), 40 George Street, Nottingham, NG1 3BG. 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.

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.

## Data subjects' rights

You have the right to:

- Information about what personal data we process, how and on what basis as set out in this policy.
- Access to your own personal data by way of a subject access request (see above).
- Correct any inaccuracies in your personal data. To do you should contact Company Directors (Data Protection), 40 George Street, Nottingham, NG1 3BG.
- 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 Company Directors (Data Protection), 40 George Street, Nottingham, NG1 3BG. 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.
- 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.
- Object if we process your personal data for the purposes of direct marketing.
- Receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.
- With some exceptions, not to be subjected to automated decision-making.
- Notified of a data security breach concerning your personal data.
- In most situations 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 your consent, you should contact Company Directors (Data Protection), 40 George Street, Nottingham, NG1 3BG. In most situations we will not rely on your consent as a lawful ground to process your data.
- Data portability which allows you to obtain and reuse your personal data for your own purposes across different services. It allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
- Complain to the Information Commissioner directly.

Further information on your rights, our obligations, exceptions to the above, and a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk).