Company Name:	Twenty-Four Seven Recruitment Services Ltd					
Policy Name:	Data Protection Policy					
Review Date:	V1 May 18	V2 28/02/22				
Reviewed and authorised by:	Amanda Lillis HR Director					

Policy Statement

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 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.

Scope

This policy applies to all personal data we process regardless of the location where that personal data is stored (e.g. on an employee's own device) and regardless of the data subject.

All individuals engaged by the Company including, volunteers and Limited Company Contractors. 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.

Staff responsibilities

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.

It is the responsibility of all individuals under scope of the policy to ensure the policy is adhered to.

Data Protection Officer responsibilities

The DPO is responsible for:

(a) advising the Company and its staff of its obligations under GDPR
(b) monitoring compliance with this Regulation and other relevant data protection law, the Company's policies with respect to this and monitoring training and audit activities relate to GDPR compliance
(c) to provide advice where requested on data protection impact assessments
(d) to cooperate with and act as the contact point for the Information Commissioner's Office
(e) the data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Third-Party Data Processors

Where external companies are used to process personal data on behalf of the Company, responsibility for the security and appropriate use of that data remains with the Company.

Where a third-party data processor is used:

(a) a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;

(b) reasonable steps must be taken that such security measures are in place;

(c) a written contract establishing what personal data will be processed and for what purpose must be set out; and,

(d) a data processing agreement, must be signed by both parties.

Policy

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 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 the 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 six 'Data Protection Principles.' It must:

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

Accountability

The Company must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The Company is responsible for, and must be able to demonstrate compliance with, the data protection principles.

We must therefore apply adequate resources and controls to ensure and to document GDPR compliance including:

1. Appointing a DPO;
2. implementing Privacy by Design when processing personal data and completing a Data Protection Impact Assessment (DPIA) where processing presents a high risk to the privacy of data subjects;
3. integrating data protection into our policies and procedures, in the way personal data is handled by us and by producing required documentation such as Privacy Notices, Records of Processing and records of Personal Data Breaches;
4. training staff on compliance with Data Protection Law and keeping a record accordingly; and
5. regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

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, your doctor, or a credit reference agency), 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 manager or other colleagues.

Data we will collect

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;
- your marital status and family details;
- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (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 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);
- a scan of your finger print for Biometric Time & Attendance Systems (where this occurs we will request your explicit consent. Your consent is voluntary and can be withdrawn at any time); and,
- any other category of personal data which we may notify you of from time to time.

How we define special categories of 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.

How we will 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 and GDPR.

We will use your personal data for:

- performing the contract of employment (or services) between us;
- complying with any legal obligation; or
- if it is necessary for our legitimate interests. However, we can only do this if your interests and rights do not override ours. You have the right to challenge our legitimate interests and request that we stop this processing.

Our "legitimate interests" for these purposes are the need to:

- Introduce candidates to our clients for permanent employment, temporary worker placements or independent professional contracts. The exchange of personal data of our candidates and our Labour User client contacts is a fundamental, essential part of this process;
- process your data to enable us to carry out the employment contract;
- gather your data for the purposes of safeguarding your health and safety;
- transfer your data intra-group for administrative purposes;
- process your data for the purposes of ensuring network and information security; and,
- protect our legal position in the event of legal proceedings.

We may from time to time need to process your sensitive personal data, such as your medical records or other information relating to your health and wellbeing. In that case we will either obtain explicit consent from you or we may consider the processing of that data as being necessary for carrying out our obligations as your employer. That will be assessed on a case-by-case basis.

We will not use your personal data for any purpose different from that for which the data was obtained in the first place 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 suffer from.

Examples of when we might process your personal data

We must process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

For example (and see section below for the meaning of the asterisks):

- 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 staff, clients and others;
- to monitor and protect the health and safety of you, our other staff, clients 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 do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information About Criminal Convictions

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you. We will use information about criminal convictions and offences usually where such processing is necessary to carry out our obligations and provided we do so in line with our contractual obligations to our clients and candidates.

Automated Decision-Making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making unless we have a lawful basis for doing so and we have notified you.

Sharing your Data

We may have to share your data with third parties, including prospective employers and third-party service providers. We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We may share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers, clients (including contractors and designated agents) and other entities within our group. The following activities are or may be carried out by third-party service providers: Payroll, Pension administration, IT services

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal information with a regulator or to otherwise comply with the law.

Transferring information outside the EU

We may transfer the personal information we collect about you outside of the EU, in order to perform our contract with you. To ensure that your personal information does receive an adequate level of protection we have put in place the appropriate measures to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects the EU and UK laws on data protection.

Marketing

As a general rule, the Company will not send promotional or direct marketing material to you

The Company may contact you for future work interests and to continue to offer you work finding services. Should you no longer wish to be considered for work you can tell us by emailing dataprotection@24-7recruitment.net and we shall cease immediately and your details shall be kept on a suppression list with a record of your opt-out decision, rather than being completely deleted.

It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

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 Retention policies.

- 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 use personal information that you hold in the course of your employment/engagement for any reason other than the performance of your duties.
- You should not share personal data informally.
- You should keep personal data secure, not on view, 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 and never share your passwords or passcodes.
- You should lock your computer screens when not at your desk.
- Personal data should be encrypted before being transferred electronically to authorised external contacts. Speak to IT for more information on how to do this.
- 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.
- Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Data Protection Officer.
- 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 Data Protection Officer.
- Personal data should be shredded and disposed of securely when you have finished with it.
- You should ask for help from our Data Protection Officer if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.
- You should immediately report any Data Breaches (such as a loss pf personal data or unauthorised access to personal data) to the Data Protection Officer.

Training

All relevant staff are trained and/or have the knowledge and skills needed to competently adhere to the policy and. The required knowledge and skills include those required to:

- Competently carry out their duties in relation to data protection,
- understand the requirements set out in current and applicable laws and guidance,
- understand the related accompanying policies, procedures and documents,
- identify data risks and consequences of not processing data correctly; and,
- understand when and how to escalate data breaches.

Data security

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used, or accessed in an unauthorised way, altered, or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality.

We have put in place procedures 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.

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.

If you are aware of a data breach you must contact the Data Protection Officer immediately at dataprotection@24-7recruitment.net and keep any evidence you have in relation to the breach.

Data Retention

We will retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. This can be found in our Data Retention Policy which is available from your local representative or the HR department.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

Subject Access Requests (SAR)

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. Such a request should be sent to the DPO 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 the Data Protection Officer at dataprotection@24-7recruitment.net We shall 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.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information
- **Request correction** of the personal information that we hold about you
- **Request erasure** of your personal information
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground
- **Request the restriction of processing** of your personal information

- **Request the transfer** of your personal information to another party

If you want to review, verify, correct, or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact Twenty-Four Seven Recruitment Services Ltd in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the HR department at Twenty-Four Seven Recruitment Services Ltd. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

You have the right to complain to the Information Commissioner. You can do this by 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.

Non compliance

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.

Review

The DPO shall review this policy every 3 years, or, where changes in legislation have occurred.