GISP LIMITED

Data Protection Policy

1 Saints Court, 5 Sylvan Hill, London, SE19 2QB, UK
Tel: +44 (0) 2086536088 Mobile: +44 (0) 7786704959 Email: enquiries@gispltd.com
Registered in England and Wales. Registered number: 7437343

Data Protection Policy

Contents

1 Purpose

1.1 We collect, store and process personal data (also referred to as personal information) relating to job applicants and about current and former employees, temporary and agency workers, contractors, interns, and volunteers for a number of specific lawful purposes, whilst carrying out our business activities.

1.2 This document is necessary to help ensure compliance with our legal obligations in respect of data processing and seeks to protect personal information relating to our workforce.

1.3 It is also intended to be a key tool toward demonstrating compliance measures to regulators and may be regarded by them as a top layer document and therefore comprises part of our layered approach to documenting practices in this area. As well as ensuring our staff understand and comply with the rules regarding the collection, use and deletion of personal information for which they may have access to, through the course of their work.

1.4 Through this policy and other practices, the organisation aims to create and operate a culture of openness in respect of data processing.

1.5 Our Data Protection Officer OR Managing Director is responsible for data protection compliance within the company. Should you have any questions or comments about this policy, or if you need further information, you should contact Managing Director. More information about the role of the Data Protection Officer OR [Job title] can be found in section 'Roles and Responsibilities'.

2 Scope

2.1 As a UK established organisation, this policy applies to all processing of personal data regardless of where in the world that processing, or any processing outsourced by us may take place.

2.2 This is an internal policy and it applies to the personal information of all job applicants, current and former employees, agency and temporary workers, contractors, interns, volunteers and any other internal persons for whom we collect, store and process personal information.

2.3 The document may be shared with third parties, contractors and other self-employed persons who will be asked to comply with the policy. Where the organisation does undertake the services of a third party, that party will be required to make adequate assurances to the data controller and/or processor that their own processing is compliant with current applicable data protection laws.

2.4 The policy applies to all data processes in general but particularly to all activities relating to the acquisition, recording, processing, sharing storing and removal of personal data. In respect of carrying out general business activities and for illustrative purposes only, such processes include but are not limited to recruitment activities, the collection of marketing data, student records, patient records, completion and protection or MAR charts.

2.5 Information that is already in the public domain is exempt from the Data Protection Act. This would include for example, information contained within externally circulated publications such as brochures and other sales and marketing literature or included on our website.

2.6 Any individual who has good reason for wishing their details not to be included in such publications should contact Managing Director.

3 Statement

We are committed to engendering a culture of accountability, integrity, and confidentiality in all aspects of the organisation regarding personal data and security. Our ultimate aim is to align every member of staff to these values such that they may be ambassadors of best practice data processing. We seek to achieve this by inducting new starters into our security practices and to maintain engagement and commitment to these values through transparent communication, providing regular training to staff and embedding privacy into our practices.

3.1.2 As an employer we process a significant amount of personal data about our staff. The type of information we require includes nationality, date of birth, contact details and medical information. The grounds upon which this information is required will include legal and contractual obligations such as demonstrating right to work checks, meeting statutory payment conditions, and corresponding with individuals in respect of their employment.

3.1.3 Please refer to section the section 'Roles and responsibilities' for the details of the Controller. For a list of your rights as a data subject, please refer to section 'The rights of data subjects'.

4 Training

4.1.1 We will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

5 Principles

5.1 All persons who process personal data with our permission must endorse and adhere to these principles at all times and especially when they obtain, handle, process, transfer, store or erase personal data.

5.2 The six fundamental principles of personal data processing are as follows:

1. Fairness, lawfulness and transparency
   All personal data must be processed fairly, lawfully and transparently.
2. Purpose limitation
   All personal data must be collected for specified, explicit and legitimate purposes and shall not be further processed in any manner that is incompatible with those purposes.
3. Data Minimisation
   All personal data must be adequate, relevant and limited to what is necessary for the purpose for which they are processed.
4. Accuracy
   All personal data must be accurate and where necessary, kept up to date with regards to the purposes. Every reasonable step to rectify or erase inaccurate personal data must be taken without delay.
5. Storage limitation

No personal data should ever be kept in a form which permits identification of a data subject for longer than is necessary to achieve the purpose.

6. Integrity and confidentiality
   All personal data must be processed in a manner that ensures appropriate security of the personal data. At the very least, it must always be protected against unauthorised or unlawful processing, accidental loss, destruction or damage, by using appropriate technical and organisational measures.

The data controller is ultimately accountable for each of these principles and is obliged by law to be able to demonstrate compliance at all times. It is for this reason that everyone in the organisation is required to take responsibility for their own strict adherence to these principles.

5.3 This policy is not contractual as it may be subject to change. However, it does indicate how we intend to meet our legal responsibilities for data protection. Therefore, any actionable points within it must be regarded as a legitimate management instruction. Explicit permission must always be sought and evidenced from a line manager before conducting yourself in a manner that varies from this policy. Failure to do so may result in disciplinary action.

5.4 We will review and update this policy in accordance with our data protection obligations. It does not form part of an employee's contract of employment, and we reserve the right to amend, update or supplement it from time to time. We will communicate any new or modified policy to employees before it is implemented. We will notify data subjects of any changes that apply to them where appropriate, personally and in writing.

6 Definitions

6.1 Personal data

Any personal information relating to a 'data subject' who can be directly or indirectly identified by reference to a piece of data, and which is processed or is intended to form part of a filing system. This applies to electronic or hard copy formats.

It includes (but is not limited to) a name, identification number, location data or online identifier. It may be an identifier that relates to physical, physiological, genetic, mental, economic, cultural, or social identity. It may also apply to data that has been pseudonymised.

The nature of the definition of data and personal data means that the expression of opinion or view about a data subject may also be regarded as personal data.

6.2 Special category data (sensitive data)

This is also more commonly referred to as 'sensitive data'. In essence this is any data that has the potential to be used to discriminate against any living (natural) person. It includes racial, ethnic, political opinion, religious or philosophical belief, trade union membership (or non-membership), genetic, biometric data (where used to identify a person), health, sex life or sexual orientation data.

It does not include information pertaining to criminal convictions however, such information must be treated with a higher level of security than generic personal data.

6.3 Data subject

An identified or identifiable, natural, legal person to whom the personal information relates.

6.4 Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is also known as a Privacy Impact Assessment (PIA). It is a method which may be used to ensure privacy by design by conducting a prescribed risk assessment on data processes and making necessary adaptations, thereby implementing appropriate safeguarding measures. A DPIA is made mandatory by law in certain circumstances.

6.5 Data protection legislation

All relevant privacy laws applicable to any personal data processed under or in connection with us, including, the UK Data Protection Act 2018, the UK General Data Protection Regulations (UK GDPR), the Privacy and Electronic Communication (EC Directive) Regulations 2003 (PECR) and all other applicable national legislation and all associated codes of practice and other guidance issued by any applicable Data Protection Authority, such as the Information Commissioner's Office (ICO).

6.6 Privacy by design

Privacy by design is the concept of ensuring that security, confidentiality, and integrity of personal data is prioritised within the heart of the methods used for processing the data.

6.7 Processing

Any activity which is performed on personal data whether or not this is manual or automated, such as: recording, organising, structuring, storing, updating, retrieving, disclosing or erasing. Examples may include sorting e-mail addresses into categories for marketing campaigns, recording absences from work, monitoring vehicle tracking etc.

6.8 Pseudonymise

To adapt how personal data is processed and presented such that the data cannot be attributed to a specific data subject, without additional personal data. The additional personal information must be kept separately and securely using appropriate technical and organisational measures.

6.9 Recipient

A natural person or organisation to whom personal data is disclosed or made available to. A recipient is not necessarily a third party with who the Company has professional dealings.

7 Handling of personal data

7.1 We will, through appropriate management and the use of strict criteria and controls:

7.1.1 observe fully the conditions concerning the fair collection and use of personal information

7.1.2 specify the purpose for which information is used

7.1.3 collect and process information only to the extent that it is needed to fulfil operational needs or legal requirements

7.1.4 endeavour always to ensure the quality of information used

7.1.5 not keep information for longer than required (operationally or legally)

7.1.6 always endeavour to safeguard personal information by physical and technical means (i.e., keeping paper files and other records or documents containing personal/sensitive data in a secure environment; protecting personal data held on computers and computer systems using secure passwords which, where possible, are changed periodically; and ensuring that individual passwords are not easily compromised)

7.1.7 ensure that personal information is not transferred outside of the EEA without suitable safeguards

7.1.8 ensure that the lawful rights of people about whom the information is held can be fully exercised.

In addition, we will ensure that:

7.2 all those who manage and handle personal information understand that they are responsible for following good data protection practice

7.3 all those who manage and handle personal information are trained to do so and appropriately supervised

7.4 a clear procedure is in place to deal with any data access requests (internal or external) that ensures that such enquiries are dealt with promptly and courteously

7.5 methods of handling personal information are regularly assessed and evaluated

7.6 any data sharing is carried out under a written agreement, setting out the scope and limits of the sharing

7.7 any disclosure of personal data will follow approved procedures.

8 Roles and responsibilities

8.1 Data Controller

Our Data Controller is Dr Hamid Rowshanaei. Their direct contact details may be found in our website.

8.1.1 The role

The Data Controller is the key decision maker in respect of why and how personal data is used and handled. The Data Controller will ensure that, both in the planning and implementation phases of processing activities, data protection principles and appropriate safeguards are addressed and implemented and that records of processing activity are kept.

8.1.2 Overview of responsibilities

- To be ultimately accountable for the Company's compliance with the six principles (see section 'Principles').

- To be able to demonstrate compliance with the six principles and therefore the proper handling and processing of all personal data. This will include information about the various data protection management resources that have been put into place and take the primary responsibility for the internal data protection framework.

- To implement appropriate technical, organisational and security measures to ensure processing is performed in accordance with data protection laws. These measures will take into account the nature, scope, context and purposes of the data processing and the risks to the rights and freedoms of individuals.

- To adopt measures to protect against any high levels of risk identified by a Privacy Impact Assessment, such as; discrimination, identity theft or significant legal, social or economic disadvantage.

- To implement internal data protection policies; assign protection responsibilities and to ensure adequate training on data protection is provided and carried out by all staff.

    - To comply with the UK GDPRs restrictions on international transfers of personal data outside of the UK.

    - Responsible for notifying data subjects as well as the Information Commission Office of personal data breaches and where necessary, any other applicable supervisory authorities within the EU (unless the breach is unlikely to result in a risk to the rights and freedoms of individuals).

    - To determine how and ensure that data subjects may exercise their rights regarding their personal data, including rights of access, rectification, erasure, restriction, data portability, objection and those related to automated decision making.

- To communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data has been disclosed unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

8.2 Data Processor

8.2.1 The role

This role processes personal data on behalf of and further to documented instruction given by the Controller.

8.2.2 Overview of responsibilities:

- To only process personal data as instructed by the Data Controller (unless otherwise required by law).
- To take all measures required to ensure their own compliance with data protection legislation regarding security.
- To make available all information necessary to demonstrate compliance with data protection legislation and to permit an audit should the Controller wish to further ensure compliance.
- To assist the controller in compliance with its obligations under data protection legislation regarding;

  - security of processing
  - assist in meeting any rights exercised by a data subject e.g. subject access request
  - notification of a personal data breach to the supervisory authority
  - communication of a personal data breach to the data subject
  - any necessary Data Protection Impact Assessments
  - consultation with the supervisory authority about any processing that should be identified as being 'high risk'

- To ensure that on instruction from the Controller, any personal data held on behalf of a client for whom we act as a processor, is deleted and returned to that client, unless we are prohibited by data protection legislation.
- To ensure data transfers outside of the UK are authorized by the Data Controller and complies with the UK GDPR transfer provisions.
- To immediately inform the Controller if it believes any instruction given by them would be in breach of data protection legislation.

Any processors are not permitted to appoint another processor without prior written agreement from the Company. Equally when we act as a processor, we will not appoint another processor without written agreement of the Controller we act on behalf of.

8.3 Data Protection Officer

8.3.1 The role

We engage Managing Director to arrange and protect the personal data we process on behalf of and in conjunction with, the Controller.

8.3.2 Overview of responsibilities

- To inform and advise the controller or the processor and the members of staff who carry out processing, of their obligations under applicable data protection legislation.
- To monitor compliance with applicable data protection legislation and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and any related audits.
- To provide advice where requested regarding any Data Protection Impact Assessments (DPIAs) and to monitor its performance.
- To cooperate with the supervisory authority when necessitated, including any consultation requirements regarding transfers.
- To perform their tasks with due regard to the risks associated with processing operations.
- To be the first point of contact for the ICO and for individuals whose data is processed.
- To not perform any tasks that may result in a conflict of interest.

9 Conditions for processing data

9.1 Under data protection legislation the processing of personal data is prohibited unless there is a legitimate legal basis upon which the data is being processed. There are six potential legal bases for processing.

9.2 In relation to any processing activity, we will, before the processing starts for the first time, and then regularly whilst it continues, review the purposes of the processing activity, and select the most appropriate lawful basis (or bases) for the processing.

9.3 Except for when the processing is on the lawful basis of consent, we will satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e., that there is no other reasonable way to achieve that purpose).

9.4 We shall document our decision as to which lawful basis applies so that we can demonstrate our compliance with the data protection principles.

9.5 Information about the purposes of the processing and the lawful basis for it, will be included in our relevant privacy notice(s).

9.6 In the processing of sensitive personal information and criminal offence information, we shall identify a lawful special condition for processing that information and document that condition.

9.7 All persons authorising the processing of personal data must be assured that at least one of the following bases applies:

9.8 Legal bases for personal data processing

9.8.1 Consent

The data subject must have given consent for specific purposes and be given the option to withdraw consent at any time. Lawful consent may only be obtained if prescribed conditions set out by data protection laws have been met. Consent must always be explicit and may not be implied.

9.8.2 Contract

The processing must be necessary to enter in to or adhere to a contract which the data subject is party to. For example, to enter into a contract of employment or when a product or service is purchased by the data subject and personal data is required to provide or perform it.

9.8.3 Legal obligation

The processing must be necessary to comply with a legal obligation that you are bound to. For example, tax obligations, evidencing the right to work or to ensure compliance with the Working Time Directive etc. Legal obligations imposed by a country outside of the UK may not be justified under this legal basis.

9.8.4 Vital interests

The processing is necessary to protect vital interests of the data subject. For example, subjects who are unable to make decisions in the best interests of their health.

9.8.5 Public interest

The processing is necessary to perform a task either in the public interest or under instruction from an official authority or regulatory body. This must be sufficient to reasonably override the interests and rights of the data subjects concerned. It may be used for the defence of a legal claim.

9.8.6 Legitimate interest

The processing must be necessary to pursue a legitimate interest, except where it is overridden by fundamental rights and freedoms of the data subject. (This is not applicable to public authorities.) When a legitimate interest is determined as a lawful basis for processing data, a record of the decision will be held and will be subject to regular review.

9.9 Special category data

The processing of special category or ‘sensitive data’ is strictly prohibited under UK data protection laws. There are limited circumstances in which it is permissible to process special category data. If any of the conditions are met, then all other conditions and protections afforded to regular personal data will also apply. Some provisions including security, should be imposed more strictly.

We will only process sensitive personal information if we have a lawful basis for doing so, as set out in section 'legal bases for personal data processing' and the data subject has been properly informed of the nature of the processing, the purpose for which it is being carried out and the legal basis for it.

Conditions under which special category data may be processed are:

9.9.1 The data subject has given explicit consent to the processing of personal data for one or more specified purposes, and there is no overriding legal prohibition.

9.9.2 Processing is necessary to carry out obligations and specific rights of the controller or of the data subject in the field of employment, social security and social protection law. Appropriate safeguards are imperative.

9.9.3 Processing is necessary to protect the vital interests of the data subject or of another person who is physically or legally incapable of giving consent. For example, in a medical emergency.

9.9.4 Processing relates to personal data which are obviously made public by the data subject.

9.9.5 Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts make instructions to the Company when acting in their judicial capacity.

9.9.6 Processing is necessary for reasons of substantial public interest, on the basis of data protection legislation. Advice from the relevant supervisory authority may need to be sought in advance to agree the appropriateness of this condition.

9.9.7 Processing is necessary for the purposes of the assessment of the working capacity of the employee recommended for care and medical industries>or for preventive or occupational medicine, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of data protection legislation, relevant legal or supervisory obligations or pursuant to contract with a health professional and subject to appropriate conditions and safeguards> .

9.10 Criminal convictions and offences

9.10.1 Personal data of this nature shall be handled with a greater level of protection than that which may be adequate for the processing of standard personal data.

9.10.2 We shall only process data of this nature where there is a legitimate requirement to do so, namely in respect of its duties as an employer. Where there is a legal obligation for the Company to review or record data of this nature an appropriate member of staff may seek to establish the required information from the employee, worker, self-employed person, contractor or any other third party.

An example of when this may be necessary include; when the performance of a duty requires a criminal record check.

9.11 Processing which does not require identification

9.11.1 When processing information, if you can remove all personal data which identifies the data subject, then you will no longer be required to adhere to the conditions for processing detailed in this policy.

9.11.2 If a data subject becomes identifiable then the conditions for processing will apply.

9.12 Retention and destruction

9.12.1 We have a policy on retention and destruction of personal data which accompanies this one, it must be adhered to by all employees, workers, contractors, and internal persons.

9.12.2 All employees are responsible for ensuring that information is not kept for longer than necessary.

9.12.3 The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Further guidance can be found in our Retention and Destruction Policy which sets out the retention periods or the criteria that should be used to determine the retention period.

9.12.4 Documents containing any personal information will be disposed of securely and paper copies will be shredded (not disposed of directly into a normal bin or recycling bin). Information stored on obsolete electronic equipment (desktops, laptops and other devices) will be erased prior to the equipment being sold, disposed of or reallocated to other employees.

10 Collecting data

10.1 Transparency principle

Anyone acting on behalf of the company is expressly required to make sure that any information they provide to a data subject or supervisory authority is done so in a manner that is: concise, transparent, intelligible, uses clear and plain language and is provided in an easily accessible form.

10.2 Collecting personal data from the subject

10.2.1 If, during your employment you are required to collect personal data, you must ensure that the data subject is advised or made aware of each of the following:

- The identity and contact details of the controller
- The purposes and legal basis of the processing
- If the legal basis is the Company's legitimate interest, the interest must be detailed
- The recipients or categories of recipients of the personal data, if any
- Whether there is an intention to transfer personal data outside the European Economic Area and if so, whether an adequacy decision exists in relation to the transfer, or alternatively reference to the appropriate or suitable safeguards relied upon by the Company and how these can be obtained

To ensure fair and transparent processing, the following information must also be provided to the data subject:

- The length of time the personal data will be stored for or the criteria used to determine the length of time it will be stored for.
- Details of their rights (see section 18).

10.3 Collecting personal data from a source other than the subject

10.4 When information of this nature is collected, the subject must be provided with all the information in the above clause as well as the information below. This should be provided at the time it is obtained, in concise and plain language:

- The categories of the personal data collected
- The source of the data (and whether it was publicly available)

10.5 In these circumstances, the information must be provided within a reasonable period after obtaining the personal data, but at the latest within one month. However, if the data shall be used to communicate with the subject, then the information must have been provided by the first communication. If it shall be disclosed to another party, then the information must have been provided by the first disclosure.

10.6 Employee records

10.7 We hold personal information about all employees as part of our general employee records. This includes address and contact details, age, date of birth, marital status or civil partnership, educational background, employment application, areas of expertise, details of salary and benefits, bank details, performance appraisals and salary reviews, records relating to holiday, sickness, and other leave, working time records and other management records. We may receive and/or retain this information in various forms (whether in writing, electronically, verbally, or otherwise).

10.8 This information is used for a variety of administration and management purposes, including payroll and benefits administration, facilitating the management of work and employees, performance, and salary reviews, complying with record keeping and other legal obligations.

10.9 We also process information relating to employees' health, some of which may fall under the definition of 'sensitive personal data'. This typically includes pre-employment health questionnaires; records of sickness absence and medical certificates (including self-certification of absence forms) night worker assessments; VDU assessments; noise assessments and any other medical reports. This information is used to administer any contractual and Statutory Sick Pay, monitor, and manage sickness absence and to comply with our obligations under health and safety legislation and the Working Time Regulations.

10.10 From time to time, we may ask employees to review and update the personal information we hold about them and will at least annually ask them to update their basic personal data. However, we ask that employees do not wait until asked to update this information but inform us immediately of any significant change(s).

10.11 Health and criminal records

10.11.1 We do not force any candidate, employee or any other data subject to provide us with access to relevant records in connection with the recruitment, continued employment or the provision of services of an individual.

10.11.2 The only exception to this is when we have another legal obligation which requires us to access the information.

10.12 Privacy and fair processing notices

10.12.1 We use privacy notices to convey the information listed in the sections above at the point of data collection.

10.13 The purpose changes

10.13.1 If the original purpose for which the data that was collected changes, then the data subject must be informed of the new purpose. They must also be informed of any changes to the information already provided under the points in this section.

10.14 Multiple controllers

10.14.1 In a situation where the Company should act jointly with other organisations as a controller, then respective responsibilities will be clearly laid out between the parties.

11 Privacy by design and by default

11.1 We embed data protection into the design of every system that uses personal data, so that it is protected throughout its entire lifecycle. To maintain this principle, all members of staff are required to:

11.2 Ensure personal data is mapped, classified into either personal or special category data, labelled, stored and accessible so that it is easily found if need be (eg in the event of a subject access request, the need to remove the data or the need to update the data).

11.3 Ensure our systems continue to function so that any personal data that is added may be deleted automatically (where appropriate).

11.4 Ensure that any new documentation which collects personal data is drafted in such a way that no personal data is requested more than what is necessary to achieve the purpose.

11.5 Ensure that a data subject is only identified for as long as necessary. This may include removing an identifier such as a name or date of birth.

11.6 Ensure that any new system will process data in a format that is commonly used.

12 Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) has been carried out in respect of processing that is considered likely to put the rights and freedoms of data subjects at a high risk.

A Data Protection Impact Assessment must always be completed if the processing of personal data is likely to be high in risk to the rights and freedoms of the data subject. Examples of processing that may be high risk include systematic monitoring of publicly accessible information on a large scale, or profiling that may significantly affect individuals.

Before any new technology or working practice is introduced, the manager responsible should contact the Managing Director in order that a DPIA can be carried out.

13 Information security

As a company we regularly review our approach to information security and stay up to date with developments in the field and emerging threats. To secure the information we hold we are committed to allocating sufficient resources (including time and budget) to ensure that robust and high-quality tools and processes are implemented.

We take all reasonable steps to protect and maintain the integrity, confidentiality, and availability of personal data. For the purposes of this policy, organisational and technological security measures are in place to protect and secure against accidental loss, damage, destruction, theft or unsanctioned disclosure, publication, or transfer of personal data.

13.1 **Protection:** All members of staff and any associated third parties are made aware of their responsibilities and are required to exercise and uphold every applicable security measure.

13.2 **Integrity:** All members of staff and any associated third parties are made aware of their responsibilities and are required to securely update and maintain completeness of personal data.

13.3 **Confidentiality:** All members of staff and any associated third parties are made aware of their responsibilities and are required to only access personal data which they are authorised to process. Those with authority to process personal data will only make personal data available to recipients (other colleagues, third parties etc) if those recipients are authorised to access or process the data.

13.4 **Availability:** We have taken measures to prevent accidental and deliberate unauthorised access. All members of staff, agency workers and any associated third parties are made aware of their responsibilities and are required to maintain the measures put in place by the Company to physically and virtually secure information. If they detect any threats to the continued availability of access to assets, systems, and information they must report this to a line manager so that it may be escalated appropriately. Threats may include damage to a computer or filing system, faulty locks, viruses, or malware.

13.5 We will also ensure that where possible, personal information is pseudonymised or encrypted and that company processes are regularly tested, assessed and evaluated on their effectiveness of technical and organisational measures for ensuring the security of processing.

13.6 This section is applicable to self-employed persons and contractors in so far as they will be asked to ensure compliance with these points and our security measures. In any event, they will be required to always uphold obligations under applicable data protection laws and without exception. Failure to do so will enable the Company to terminate the service agreement without notice and the incident may be reported to the relevant supervisory authority.

14 External organisations

14.1 Where we use external organisations to process personal information on our behalf, we will implement additional security arrangements in contracts with those organisations to safeguard the security of personal information. We will ensure contracts with external organisations will provide:

14.1.1 the organisation may act only on our written instructions;

14.1.2 those processing the data are subject to a duty of confidence;

14.1.3 appropriate measures are taken to ensure the security of processing;

14.1.4 sub-contractors are only engaged with our prior consent and under a written contract;

14.1.5 the organisation will assist us in providing subject access and allowing individuals to exercise their rights in relation to data protection;

14.1.6 the organisation will assist us in meeting our obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;

14.1.7 the organisation will delete or return all personal information to us as requested at the end of the contract; and

14.1.8 the organisation will submit to audits and inspections, provide us with whatever information we need to ensure that we are both meeting our data protection obligations, and tell us immediately if it is asked to do something infringing data protection law.

14.2 Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the Managing Director.

15 Transferring personal data to a country outside the EEA

15.1 Caution must be taken before any personal data is ever transferred outside of the EEA. Refer to the paragraphs below. Contact us for advice and further information.

15.2 We may transfer personal data outside of the EEA in respect of any employees, workers, self-employed persons, contractors or any other third parties operating on behalf of the Company. Where this is the case, the transfer is made because it is necessary for the performance of the contract between us and the individual.

15.3 As we may need to transfer personal data outside of the European Economic Area ("EEA"), we have ensured that the following condition(s) apply:

- The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- The Company has appropriate safeguards which support the rights of data subjects.
- The transfer is necessary for one of the reasons set out in data protection legislation, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims or for compelling legitimate interests.
- The transfer is authorised by the relevant data protection authority.
- Binding Corporate Rules (BCR), the data subject must be provided with information about the principles contained in the BCR, their rights and how these may be exercised, how compensation may be obtained for a breach of the BCR and the liability arrangements in the BCR.

15.4 Subject to the above, personal data we hold may be processed by staff operating outside the EEA who work for us or for one of our suppliers. These staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

15.5 The data subject will be informed of the possible risks of the transfer due to the absence of an adequacy decision and an explanation of the appropriate safeguards taken, the reason(s) for the transfer and their associated rights.

16 Record keeping

There is a legal requirement for employers to keep records about processing activities which are carried out regarding the employment of staff e.g. recruitment processes, onboarding, employee relations, leaver processes, payroll etc. Other areas of your business using personal data may also require records of processing activities to be kept as per the bullet points below.

We maintain records of data processing activities in accordance with data protection legislation. Internal records are kept regarding data processes which are carried out regarding the employment of our staff.

Record keeping is also carried out for the following activities:

- Processing of personal data which is likely to result in a risk to the rights and freedoms of data subjects
- Processing of personal data which is regular and frequent
- Processing of personal data which includes special category data
- Processing of personal data which includes data about criminal convictions

17 Breach and incident reporting

17.1 Serious breaches must be reported to the relevant supervisory authority within 72 hours of becoming aware of the breach. Therefore, all employees and workers must immediately report an incident that may potentially or actually put personal data at risk of a data breach. This is never more imperative than when it is suspected that there may be actual loss, theft unauthorised disclosure or inappropriate use of personal data, either wholly or partly. In this event you must immediately refer to and follow the Company's Breach and Incident and Reporting Procedure.

17.2 Anyone who reports any incident or breach of data protection which amounts to a protected disclosure, will be protected in accordance with the Company’s Whistleblowing Policy.

17.3 Where a third-party service provider notifies you of an incident that may affect the Company and its responsibilities, you must immediately report the incident. In this event you must immediately refer to and follow the Company's Breach and Incident Reporting Procedure.

18 The rights of data subjects

18.1.1 We shall be diligent in providing data subjects information about their rights and in complying with any appropriate assertions of their rights.

18.1.2 All reasonable efforts will be made to verify the identity of the data subject before carrying out any requests or disclosures of information made by them. These efforts may include the request for additional personal information if necessary.

18.1.3 The following rights apply to all data subjects:

18.1.3.1 **Right to be informed**: to be informed about how, why and on what basis that information is processed

18.1.3.2 **Right of access**: to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request.

18.1.3.3 **Right to rectification**: to have data corrected if it is inaccurate or incomplete

18.1.3.4 **Right to erasure (right to be forgotten)**: to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed or if there are no overriding legitimate grounds for the processing

18.1.3.5 **Right to restriction of processing**: to restrict the processing of information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data erased), or where the employer no longer needs the personal information but you require the data to establish, exercise or defend a legal claim

18.1.3.6 **Right to not be subject to automatic decision making**: We will not carry out automated decision making including profiling, based on an individual's sensitive personal information.

18.1.3.7 Right to object: To restrict the processing of personal information where you have objected to the processing and the employer is considering whether the organization's legitimate grounds override your interests.

18.1.3.8 **Right to data portability**: to allow individuals to obtain a copy of their personal data and/or have their personal data transmitted from one controller to another controller.

19 Subject access requests

19.1 Making a request

19.1.1 If you wish to make a subject access request to verify the lawfulness and accuracy of the personal data we hold about you, then you are encouraged to put your request in writing (letter or e-mail) and submit it to Managing Director.

19.1.2 Your request should be specific about the nature and the type of data you require.

19.1.3 Every attempt will be made to comply with your request in a timely manner and without undue delay.

19.1.4 Upon receipt of the information, you are encouraged to check the accuracy of the information and to advise the Company of any updates that may need to be made.

19.1.5 A fee will not be charged for an access request, except where a request is deemed to be 'manifestly excessive' or you have already been provided with the information.

19.2 Receiving a request

19.2.1 If you receive a request, you should pass it to the Managing Director immediately.

19.2.2 Requests must be acknowledged upon receipt.

19.2.3 Requests must be complied with in a timely manner and without undue delay. If it is anticipated that compliance with a request is not going to be immediate then the Controller should be notified and informed of the legitimate reasons for this. The information requested must be provided within one month of receipt of the request.

19.2.4 If an extension to the time line is absolutely necessary under exceptional circumstances, then any extension must be agreed by the data subject and signed off by the Controller one month of the request. If an extension is agreed, then the information must be provided within a maximum of three months from the receipt of the request.

19.2.5 If a request is received electronically (eg via e-mail) then the request must be responded to electronically.

19.2.6 The data must be provided in a common format (eg a paper file, a pdf document etc.).

19.2.7 Only personal data pertaining to the individual who made the request should be released.

19.2.8 If there is any doubt over the identity of the individual making the access request, then reasonable steps must be taken to verify their identity, before complying with the request.

19.2.9 When the personal data is provided, the individual must be informed of the right to lodge a complaint with the relevant supervisory authority and the existence of the right to objection, rectification, erasure and restriction of the data.

19.2.10 The data subject may be directed to the relevant privacy/fair processing notice which will provide advice on the conditions for processing.

19.2.11 If requested, the following information must be provided as part of the response:

- The purpose of the data
- The categories of data that which are held
- The recipients of the data (past, present and intended in the future)
- The criteria that determine how long the data is retained for
- The source of the data if not collected from the individual directly

20 General guidance for employees

20.1 We recognise that there are different areas in the organisation where members of staff may be responsible for processing personal data in different ways. We also recognise that responsibilities and nuances in processing are likely to vary across specialisms and levels of seniority.

20.2 We will provide guidance to staff when processing personal data specific to their job. This information shall include:

- A description of the limitations which surround how personal data can be used.
- The steps that must be followed to ensure that personal data is maintained accurately.
- A comprehensive discussion of security obligations, including all reasonable steps that should be taken as a minimum to prevent unauthorised access or loss.
- Confirmation of whether the transfer of personal data shall be permitted. Transfer of personal data is prohibited unless specific legitimate grounds have been established.
- Specific information regarding the way in which personal data should be handled when it is destroyed or deleted.

21 General responsibilities of management

21.1 All members of the senior management are responsible for championing and enforcing this policy to all other staff within the Company, whenever appropriate.

21.2 Particular roles within senior management are responsible for assessing the business risk arising as a result of processing personal data. These roles include: CEO & Head of Operation.

21.3 Those members of senior management identified above are required to work with the Company to develop procedures and controls to identify and address risks appropriately.

21.4 Responsibility will be allocated to individual roles for determining risk-based technical, physical and administrative safeguards including safeguards for equipment, facilities and locations where personal data is stored; establishing procedures and requirements for collecting, transporting, processing, storing, transferring (where appropriate) and destroying personal data. These considerations must also be given when dealing with any third parties who may be authorised or obligated to process personal data on behalf of the Company.

22 Non-compliance

22.1 This policy along with associated documents, seeks to guide and instruct all member of staff on how they ensure compliance with data protection laws to which the Company is subject.

22.2 If a member of staff should fail to comply with applicable data protection laws, they may subject the Company and themselves as individuals to civil and criminal penalties. This is likely to jeopardise the reputation of the Company and as a result may impact on the operational and performance capabilities of the business.

22.3 As the ramifications of non-compliance are potentially severe, any failure to comply with this policy or reasonable instruction given in connection with the protection and security of personal data, may result in disciplinary action. Serious, deliberate or negligent transgressions may be regarded as gross misconduct and if substantiated, may result in summary dismissal (without notice).

22.4 Third parties, contractors and self-employed persons

22.4.1 If any self-employed person, contractor or third party, such as agency staff, are found to be failing to meet obligations with applicable data protection laws then notice may be served on the contract for service.

22.4.2 Serious, deliberate, or negligent transgressions may permit us to terminate the contract with immediate effect. In this event, all reasonable steps will be taken to recover and protect the personal data concerned and the relevant supervisory authority will be notified. Where the rights and freedoms of data subjects are likely to be at risk, the data subjects will be notified without delay.

23 Related policies and documents

- Data retention guidelines
- Record keeping policy
- Disciplinary policy
- Information security policy
- IT policy
- Personal Data Policy
- Social media policy

The above list is not exhaustive.

24 Further information

Any queries or comments about this policy, or any concerns that the policy has not been followed, should be addressed to Dr H. Rowshanaei

25 Policy owner

This policy is owned and maintained by our Managing Director.

Date last reviewed: 12/03/2022

Approved by:

Managing Director

Dr H. E. Rowshanaei