Data Breach Notification Procedure

1. Purpose

The Company (“we”/”us”) have this procedure in place to provide a standardised response to any reported data breach incident and ensure that data breaches are appropriately logged and managed in accordance with the law and best practice.

2. Scope

This procedure applies in the event of a personal data breach and applies to all employees at all times, and whether located within the physical offices or not.

The document applies to all information we hold and all information technology systems utilised by us.

3. Responsibility

3.1 All employees/Staff, contractors or temporary employees/staff and third parties working for or on behalf of us are required to be aware of, and to follow this procedure in the event of a personal data breach.

3.2 All Employees/Staff, contractors or temporary personnel are responsible for reporting any personal data breach to Michael Salvador whose contact details are as follows:

Telephone: 07851666969
Email: michael@makiramen.com

4. Definition

The UK GDPR defines a “personal data breach” in Article 4(12) as: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”. Examples include:

- Loss or theft of data or equipment on which data is stored
- Access by an unauthorised third party
- Sending personal data to an incorrect recipient
- Alteration of personal data without permission

- Loss of availability of personal data such as equipment failure
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceit for the purposes of this procedure data security breaches include both confirmed and suspected incidents.

*If you suspect a data breach or are unsure whether the incident which has occurred constitutes a data breach please refer the matter to the *DPO* for consideration*

5. Reporting an incident

5.1 Any individual who accesses, uses or manages information within our business is responsible for reporting data breach and information security incidents immediately to the *DPO.*

5.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

5.3 The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, the nature of the information, and how many individuals are involved.

6. Next Steps

6.1 The *DPO* will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

6.2 An initial assessment will be made by the *DPO* in liaison with relevant persons (which may include IT services) to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach).

6.3 An investigation will be undertaken immediately and wherever possible within 24 hours of the breach being discovered/reported.

6.4 The *DPO* will investigate the risks associated with the breach, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

6.5 The *DPO* will then establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

6.6 The *DPO* will identify who may need to be notified. The relevant procedures from those identified below will then be followed. Every incident will be assessed on a case by case basis.

7. Procedure – Breach notification data processor to data controller

7.1 The Company must report any personal data breach or security incident to the data controller without undue delay. These contact details are recorded in the Internal Breach Register. The Company provides the controller with all of the details of the breach.

7.2 The breach notification should be made by *email or phone call.*

7.3 A confirmation of receipt of this information should be requested and made by *email or*

phone call.

8. Procedure – Breach notification data controller to supervisory authority

8.1 The *DPO* will determine if the supervisory authority (the Information Commissioner's Office (ICO) in the UK) need to be notified in the event of a breach.

8.2 If the breach affects individuals in different EU countries, the ICO may not be the lead supervisory authority. The *DPO* will also need to establish which European data protection agency would be the lead supervisory authority for the processing activities that have been subject to the breach.

8.3 We will assess whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach, by conducting an investigation and/or an impact assessment. If we decide that we do not need to report the breach to the ICO we will justify and document our decision.

8.4 If a risk to data subject(s) is likely, the *DPO* will report the personal data breach to the ICO without undue delay, and not later than 72 hours after becoming aware of it.

8.5 If the data breach notification to the ICO is not made within 72 hours, *the DPO* will submit notification electronically with a justification for the delay.

8.6 If it is not possible to provide all of the necessary information at the same time we will provide the information in phases without undue further delay.

8.7 The following information needs to be provided to the supervisory authority:

8.7.1 A description of the nature of the breach.

8.7.2 The categories of personal data affected.

8.7.3 Name and contact details of the *DPO*.

8.7.4 Likely consequences of the breach.

8.7.5 Any measures taken to address the breach.

8.7.6 Any information relating to the data breach.

8.7.7 Approximate number of data subjects affected.

8.7.8 Approximate number of personal data records affected.

8.8 The breach notification should be made via telephone - ICO: 0303 123 1113. Alternatively, if the *DPO* may choose to report it online if they are still investigating and will be able to provide more information at a later date or if they are confident that the breach has been dealt with appropriately.

8.9 In the event the ICO assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register.

9. Procedure – Breach notification data controller to data subject

9.1 If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, we will notify those/the data subjects affected without undue delay and in accordance with the *DPO's* recommendation.

9.2 A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. In any event the *DPO* will document their decision-making process.

9.3 We will describe the breach in clear and plain language, in addition to information specified in clauses 8.7.1-8.7.6 above.

9.4 The data controller takes subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur.

9.5 If the breach affects a high volume of data subjects and personal data records, we will make a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder our ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure informs those affected in an equally effective manner and will be considered by the *DPO* whose decision will be final.

9.6 If we have not notified the data subject(s), and the supervisory authority considers the likelihood of a data breach will result in high risk, we will communicate the data breach to the data subject by telephone or email.

9.7 We will document any personal data breach(es) within the Data Breach Register, incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.

10. Documentation requirements

Internal breach register: there is an obligation for us to document each incident "comprising the facts relating to the personal data breach, its effects and the remedial action taken".

11. Evaluation

11.1 Once the initial incident is contained, the *DPO* will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

11.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

11.3 The review will consider various points, including but not limited to:

- Where and how personal data is held and where and how it is stored
- Where the biggest risks lie, and will identify any further potential weak points within its existing measures
- Whether methods of transmission are secure; sharing minimum amount of data necessary Identifying weak points within existing security measures
- Staff awareness

Data Protection (Employment) Policy

1 Introduction and scope

1.1 The Company obtains, keeps and uses personal information (also referred to as data) about job applicants and about current and former staff for a number of specific lawful purposes as set out in the Company's data protection privacy notices.

1.2 For the purposes of this policy, staff include: employees, workers, consultants, contractors, volunteers and apprentices.

1.3 This policy is non-contractual and the Company may amend it at any time. The Company will also review, and if necessary update, this policy in accordance with our data protection obligations.

1.4 This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our workforce. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

2 Definitions

Criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
Data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
Data subject	means the individual to whom the personal information relates;
Personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
Processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
Pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
Sensitive personal information	(sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

3 Data protection principles

3.1 The Company will comply with the following data protection principles when processing personal information:

3.1.1 we will process personal information lawfully, fairly and in a transparent manner;

3.1.2 we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

3.1.3 we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;

3.1.4 we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;

3.1.5 we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and

3.1.6 we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

4 Basis for processing personal information

4.1 In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

4.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:

(a) that the data subject has consented to the processing;

(b) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) that the processing is necessary for compliance with a legal obligation to which the Company is subject;

(d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person; or

(e) that the processing is necessary for the purposes of legitimate interests of the Company or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.

4.1.2 except where the processing is based on consent, 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);

4.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

4.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

4.1.5 where sensitive personal information is processed, also identify a lawful special condition for processing that information (see paragraph 5.1.2 below), and document it; and

4.1.6 where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

5 Sensitive personal information

5.1 The Company may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

5.1.1 we have a lawful basis for doing so as set out in paragraph 4.1.1 above; and

5.1.2 one of the special conditions for processing sensitive personal information applies, e.g.:

(a) the data subject has given has given explicit consent;

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject;

(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

(d) processing relates to personal data which are manifestly made public by the data subject;

(e) the processing is necessary for the establishment, exercise or defence of legal claims; or

(f) the processing is necessary for reasons of substantial public interest.

5.2 Before processing any sensitive personal information, staff must notify Michael Salvador of the proposed processing so that they may assess whether the processing complies with the criteria noted above.

5.3 Sensitive personal information will not be processed until the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

5.4 The Company will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.

6 Data protection impact assessments (DPIAs)

6.1 Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the Company is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

6.1.1 whether the processing is necessary and proportionate in relation to its purpose;

6.1.2 the risks to individuals; and

6.1.3 what measures can be put in place to address those risks and protect personal information.

6.2 During the course of any DPIA, the employer will, where appropriate, seek the views of employees (this may be a representative group) and any other relevant stakeholders.

7 Documentation and records

7.1 We will keep written records of processing activities which are high risk, i.e. which may result in a risk to individuals' rights and freedoms or involve sensitive personal information or criminal records information.

7.2 As part of our record of processing activities we document, or link to documentation, on:

7.2.1 information required for privacy notices;

7.2.2 records of consent;

7.2.3 controller-processor contracts;

7.2.4 the location of personal information;

7.2.5 DPIAs; and

7.2.6 records of data breaches.

7.3 We may document our processing activities in electronic form so we can add, remove and amend information easily.

8 Individual rights

8.1 You (in common with other data subjects) have the following rights in relation to your personal information:

8.1.1 to be informed about how, why and on what basis that information is processed—see the Company's data protection privacy notices;

8.1.2 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—see section Subject access requests below;

8.1.3 to have data corrected if it is inaccurate or incomplete;

8.1.4 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 (this is sometimes known as 'the right to be forgotten');

8.1.5 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information but you require the data to establish, exercise or defend a legal claim; and

8.1.6 to restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).

8.2 If you wish to exercise any of the rights in paragraph 9.1, please contact Michael Salvador.

9 Subject access requests

9.1 Data subjects have the right to request access to their personal data processed by us. Such requests are called subject access requests (SARs). When a data subject makes an SAR, we will usually take the following steps:

(a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

(b) confirm the identity of the data subject who is the subject of the personal data. For example, we may request additional information from the data subject to confirm their identity;

(c) search databases, systems, applications and other places where the personal data which are the subject of the request may be held; and

(d) confirm to the data subject whether or not personal data of the data subject making the SAR are being processed.

9.2 If personal data of the data subject are being processed, we shall provide the data subject with the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other (including electronic) means:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients overseas;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data or to object to such processing;

(f) the right to lodge a complaint with the Information Commissioner's Office (ICO);

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and

(i) where personal data are transferred outside the EU, details of the appropriate safeguards to protect the personal data.

9.3 We shall also, unless there is an exemption, provide the data subject with a copy of the personal data processed by us in a commonly used electronic form (unless the data subject either did not make the request by electronic means or has specifically requested not to be provided with the copy in electronic form) within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the

period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

9.4 Before providing the personal data to the data subject making the SAR, we shall review the personal data requested to see if they contain the personal data of other data subjects. If they do, we may redact the personal data of those other data subjects prior to providing the data subject with their personal data, unless those other data subjects have consented to the disclosure of their personal data.

9.5 If the SAR is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing the personal data, or refuse to act on the request.

9.6 If we are not going to respond to the SAR we shall inform the data subject of the reason(s) for not taking action and of the possibility of lodging a complaint with the ICO.

10 Individual obligations

10.1 You may have access to the personal information of other members of staff, suppliers and customers or clients of the Company in the course of your employment or engagement. If so, the Company expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out in paragraph 9.1 above.

10.2 If you have access to personal information, you must:

10.2.1 only access the personal information that you have authority to access, and only for authorised purposes;

10.2.2 only allow other Company staff to access personal information if they have appropriate authorisation;

10.2.3 only allow individuals who are not Company staff to access personal information if you have specific authority to do so from Michael Salvador.

10.2.4 keep personal information secure;

10.2.5 not remove personal information, or devices containing personal information (or which can be used to access it), from the Company's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and

10.2.6 not store personal information on local drives or on personal devices that are used for work purposes.

10.3 You should contact Michael Salvador if you are concerned or suspect that any breaches of this policy have taken place (or is taking place or likely to take place).

11 Information security

11.1 Information may be held at our offices and third party agencies, service providers, representatives and agents and in cloud based IT services.

11.2 The Company will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

11.2.1 making sure that, where possible, personal information is pseudonymised or encrypted;

11.2.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

11.2.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and

11.2.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

11.3 Where the Company uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. 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 Michael Salvador.

12 Retention of personal (and sensitive personal) information

12.1 Personal information (and sensitive personal information) will be retained in accordance with Schedule 1.

12.2 Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

13 Data breaches

13.1 A data breach may take many different forms, for example:

13.1.1 loss or theft of data or equipment on which personal information is stored;

13.1.2 unauthorised access to or use of personal information either by a member of staff or third party;

13.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

13.1.4 human error, such as accidental deletion or alteration of data;

13.1.5 unforeseen circumstances, such as a fire or flood;

13.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

13.1.7 ‘blagging’ offences, where information is obtained by deceiving the organisation which holds it.

13.2 The Company will:

13.2.1 make the required report of a data breach to the Information Commissioner’s Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

13.2.2 notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

14 Consequences of failing to comply

14.1 The Company takes compliance with this policy very seriously. Failure to comply with the policy puts individuals whose personal information is being processed at risk, carries significant civil and criminal sanctions for the individual and the Company and may, in some circumstances, amount to a criminal offence by the individual.

14.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

14.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact Michael Salvador.

Schedule 1

Type of employment record	Retention period
Recruitment records including but not limited to: ● Completed online application forms or CVs. ● Equal opportunities monitoring forms. ● Assessment exercises or tests. ● Notes from interviews and short-listing exercises. ● Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references. (These may be transferred to a successful candidate's employment file.)	Six months after notifying candidates of the outcome of the recruitment exercise.
Immigration checks	Two years after the termination of employment.

Contracts	While employment continues and for six years after the contract ends.

Payroll and wage records	
PAYE records	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for six years after employment ends.
Other payments	While employment continues and for six years after employment ends.
Records in relation to hours worked and payments made to workers	These must be kept for three years beginning with the day on which the pay reference period immediately following that to which they relate ends. However, given their potential relevance to pay disputes they will be retained for six years after the working relationship ends.
Current bank details	Bank details will be deleted as soon after the end of employment as possible once final payments have been made.
Payroll and wage records for companies	These must be kept for six years from the financial year-end in which payments were made. However, given their potential relevance to pay disputes they will be retained for six years after employment ends.

Personnel records	
These may include: ● Qualifications/references. ● Consents for the processing of special categories of personal data.	While employment continues and for six years after employment ends.

● Annual leave records. ● Annual assessment reports. ● Disciplinary procedures. ● Grievance procedures. ● Death benefit nomination and revocation forms. ● Resignation, termination and retirement. ● Working Time Opt Outs	
Records in connection with working time	
Records to show compliance	Two years after the relevant period.
Maternity records	
These may include: ● Maternity payments. ● Dates of maternity leave. ● Period without maternity payment. ● Maternity certificates showing the expected week of confinement.	Three years after the end of the tax year in which the maternity pay period ends.

Accident records	
These are created regarding any reportable accident, death or injury in connection with work.	For at least three years from the date the report was made.

Data Protection Privacy Notice

This non-contractual notice explains what personal data (personal information) we hold about you, how we collect it, and how we use and may share personal information during your employment and after it ends. Please ensure that you read this notice and any other similar notice we may provide to you from time to time.

Who collects the personal information

The Company is a 'data controller' and gathers and uses certain personal information about you.

Data protection principles

The data protection principles which we will apply when gathering and using personal information are set out in our Data Protection Policy.

About the personal information we collect

A table summarising the personal information we collect and hold, how and why we do so, how we use it and with whom it may be shared is below.

Personal information may be shared with other parties, such as group companies and/or affiliated companies, external contractors and our professional advisers (e.g. legal and financial advisors), HR advisors and payroll providers, and potential purchasers of some or all of our business or on a re-structuring. The recipient of the personal information will be bound by confidentiality obligations. We may also be required to share some personal information to comply with the law. We seek to ensure that our personal information collection and processing is always proportionate. We will notify you of any material changes to personal information we collect or to the purposes for which we collect and process it.

Where personal information may be held

Personal information may be held at our offices and third-party agencies, service providers, representatives and agents as described above and in cloud based IT services. In the event that we use cloud based IT services, personal information may be transferred internationally to other countries around the world, including countries that do not have data protection laws equivalent to those in the UK. We have security measures in place to seek to ensure that there is appropriate security for personal information we hold.

How long we keep your personal information

We keep personal information during and after your employment for no longer than is necessary and in the majority of cases for no more than 6 years after the end of your employment.

Your rights to correct and access your personal information and to ask for it to be erased

Please contact our Data Protection Contact Michael Salvador if (in accordance with applicable law) you would like to correct or request access to personal information that we hold or if you have any questions about this notice. You also have the right to ask our Data Protection

Contact for some, but not all, of the personal information we hold and process to be erased (the ‘right to be forgotten’) in certain circumstances

Keeping your personal information secure

We have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing personal information will do so only in an authorised manner and are subject to a duty of confidentiality. We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

How to complain

We hope that we can resolve any query or concern you raise about our use of your personal information. If not, contact the Information Commissioner at ico.org.uk/concerns/ or telephone: 0303 123 1113 for further information about your rights and how to make a formal complaint.

Key to table below

Access – to monitor/manage staff access to our systems and to record staff absences GEP – to maintain employment records and for good employment practice
Insurance - to comply with the terms of our insurance
LO – to ensure compliance with legal and/or regulatory obligations
Medical Professional – your doctors and other medical/occupational health professionals
Policies – to ensure compliance with our policies, such as EOP and sickness absence
Protect – to protect our networks and personal data of employees and customers/clients

PTC – to enter into/perform the contract

Personnel – relevant managers, HR, professional advisors, payroll and consultants
SA – for staff administration
SPI - for reasons of substantial public interest (e.g. equal opportunities, prevention and/or detection of unlawful acts)
SWP – to ensure safe working practices

The information we collect	**How we collect the information**	**Why we collect the information (including legitimate interest)**	**How we use and may share the information**
Your name, contact details (including emergency contact), other employment records *	From you	PTC, GEP	PTC, SA Share: Personnel
Financial details (e.g. salary, benefits, bank, NI, tax information), your spouse/partner,	From you	PTC, GEP	PTC Share: Personnel, HMRC, our bank

dependants, your age *			
Your qualifications and any professional status *	From you	PTC, GEP	PTC Share: Personnel, clients (if required)
Your nationality and immigration status and information from related documents (e.g. passport) *	From you, the Home Office (if required)	PTC, GEP	PTC Share: Personnel, the Home Office (if required)
Pension arrangements and all information necessary to implement and administer them *	From you, pension administrators	PTC	PTC Share: Personnel, pension administrators, HMRC
Sickness and absence records (including sensitive personal information regarding your physical and/or mental health) *	From you, Medical Professionals, any insurance benefit administrators	PTC, GEP and SWP	PTC, LO Share: Personnel, Medical Professionals, any insurance benefit administrators †
Trade Union (TU) membership	From you, your TU	PTC, GEP	PTC Share: Personnel, your TU
Information on grievances & conduct issues	From you, other employees, consultants, any interested third parties	PTC, LO, GEP, SWP	PTC Share: Personnel, any interested third parties (if appropriate)
Details of your performance (e.g. appraisals)	From you, other employees, consultants	PTC, LO, GEP, SWP	PTC Share: Personnel
Time and attendance records (including biometric data where the system requires this †)	From you, any time recording system	PTC, access	PTC Share: Personnel
Your use of our	Websites, applications,	PTC, Access,	See adjacent

systems and your actions in and around the work place	other technical systems (e.g. CCTV, phone, email, internet)	Protect, Policies, operational reasons, statistical analysis	column Share: Personnel, any interested third parties
Your use of public social media (only in very limited circumstances to check specific risks for specific functions within our organisation) and any business related social media (e.g. LinkedIn)	Websites, applications	PTC, protect our external reputation, adherence to restrictions and policies	See adjacent column Share: Personnel
Photographs	From you	ID documents, marketing	PTC, promote the company Share: website, promotional material
Details in references about you that we give to others	From your personnel records, other employees	PTC, LO, GEP	To provide a reference Share: Personnel and the recipient(s) of the reference

You are required (by law or under the terms of your contract of employment, or in order to enter into your contract of employment) to provide the categories of information marked '*' above to us to enable us to verify your right to work and suitability for the position, to pay you, to provide you with your contractual benefits and to administer statutory payments such as statutory sick pay (SSP). If you do not provide this information, we may not be able to employ you, make these payments or provide these benefits.

† Further details on how we handle sensitive personal information are set out in our Data Protection Policy.

Data protection privacy notice (recruitment)

This non-contractual notice explains what personal data (personal information) we hold about you, how we collect it, and how we use and may share personal information during the recruitment process. Please ensure that you read this notice and any other similar notice we may provide to you from time to time.

Who collects the personal information

The Company is a 'data controller' and gathers and uses certain personal information about you.

Data protection principles

The data protection principles which we will apply when gathering and using personal information are that:

1. we will process personal information lawfully, fairly and in a transparent manner;
2. we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
3. we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;
4. we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
5. we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and
6. we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

About the personal information we collect

A table summarising the personal information we collect and hold during the recruitment process, how and why we do so, how we use it and with whom it may be shared is below.

Where personal information may be held

Personal information may be held at our offices and third-party agencies, service providers, representatives and agents as described above and in cloud based IT services. In the event that we use cloud based IT services, personal information may be transferred internationally to other countries around the world, including countries that do not have data protection laws equivalent to those in the UK. We have security measures in place to seek to ensure that there is appropriate security for personal information we hold.

How long we keep your personal information

We keep the personal information that we obtain about you during the recruitment process for no longer than is necessary. How long we keep your personal information will depend on whether your application is successful, and you become employed by us, the nature of the personal information concerned and the purposes for which it is processed.

If your application is successful, we will keep only the recruitment personal information that is necessary in relation to your employment. For further information, see *our data protection privacy notice (employment)*.

Your rights to correct and access your personal information and to ask for it to be erased
Please contact our Data Protection Contact Michael Salvador if (in accordance with applicable law) you would like to correct or request access to personal information that we hold or if you have any questions about this notice. You also have the right to ask our Data Protection Contact for some, but not all, of the personal information we hold and process to be erased (the 'right to be forgotten') in certain circumstances.

Keeping your personal information secure
We have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing personal information will do so only in an authorised manner and are subject to a duty of confidentiality. We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

How to complain
We hope that we can resolve any query or concern you raise about our use of your personal information. If not, contact the Information Commissioner at ico.org.uk/concerns/ or telephone: 0303 123 1113 for further information about your rights and how to make a formal complaint.

Key to table below
FRP – to carry out a fair recruitment process
GEP – to maintain employment records and for good employment practice
Informed - to make an informed decision to shortlist for interview and (if relevant) to recruit
Insurance - to comply with the terms of our insurance
LO – to ensure compliance with legal and/or regulatory obligations
Medical Professional – your doctors and other medical/occupational health professionals PTC – to enter into/perform the contract
Personnel – relevant managers, HR, professional advisors, payroll and consultants
Progress - to progress your application, arrange interviews and inform you of the outcome at all stages
SPI - for reasons of substantial public interest (e.g. equality opportunities and prevention and/or detection of unlawful acts)

The information we collect	How we collect the information	Why we collect the information (including legitimate interest)	How we use and may share the information
Your name, contact details (including	From you	FRP, Progress	Progress, Shared with Personnel

emergency contact), other employment records ☐			
Details of your academic history qualifications, experience, employment history (including job titles, salary and working hours) and interests	From you, in the completed application form and interview notes (if relevant)	FRP, Informed	Informed Shared with Personnel
Your nationality and immigration status and information from related documents (e.g. passport) ☐	From you, the Home Office (if required)	PTC, GEP, LO	To carry out right to work checks Share: Personnel, the Home Office (if required)
Medical, sickness and absence records (including sensitive personal information regarding your physical and/or mental health) ☐	From you, Medical Professionals, any insurance benefit administrator s	LO & SPI	Share: Personnel, Medical Professionals, any insurance benefit administrators*

You are required (by law or in order to enter into your contract of employment) to provide the categories of information marked '□' above to us to enable us to verify your right to work and suitability for the position.

* Sensitive Personal Information

Before processing any sensitive personal information, staff must notify the Data Protection Contact of the proposed processing, in order that the Data Protection Contact may assess whether the processing complies with the special conditions for processing sensitive personal information.