

DATA PROTECTION & GDPR POLICY

Designated Officer:	Barry Pactor
Designated Officer Contact details:	020 3773 4144
Date:	October 2023
Review Date:	October 2024
Policy review schedule:	Every 12 months
Document Ref:	CJH10012/5

Introduction

All organisations that process *personal data* are required to comply with data protection legislation. This includes in particular the Data Protection Act 1998 (or its successor) and the EU General Data Protection Regulation (together the 'Data Protection Laws'). The Data Protection Laws give individuals certain rights over their *personal data* whilst imposing certain obligations on the organisations that process their data.

As a recruitment business the Company collects and processes both *personal data* and *sensitive personal data*. It is required to do so to comply with other legislation. It is also required to keep this data for different periods depending on the nature of the data.

This policy sets out the Company's procedures for implementing the Data Protection Laws. It should be read in conjunction with the REC's model Data Protection Policy.

Definitions

In this policy the following terms have the following meanings:

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

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

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

'personal data'* means any information relating to an individual who can be identified, such as by a name, an identification number, location data, an online identifier or to one or more factors

specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

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

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

'profiling' means any form of automated *processing of personal data* consisting of the use of *personal data* to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

'pseudonymisation' means the *processing of personal data* in such a manner that the *personal data* can no longer be attributed to an individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the *personal data* are not attributed to an identified or identifiable individual;

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

* For the purposes of this policy we use the term '*personal data*' to include '*sensitive personal data*' except where we need to refer to *sensitive personal data* specifically.

'supervisory authority' means an independent public authority which is responsible for monitoring the application of data protection. In the UK the *supervisory authority* is the Information Commissioner's Office (ICO).

All of these definitions are italicised throughout this policy to remind the reader that they are defined terms.

Data processing under the Data Protection Laws

The Company processes *personal data* in relation to its own staff, work-seekers and individual client contacts and is a *data controller* for the purposes of the Data Protection Laws.

The Company may hold *personal data* on individuals for the following purposes:

- Staff administration;
- Accounts and records;

- Administration and *processing* of work-seekers' *personal data* for the purposes of providing work-finding services, including *processing* using software solution providers and back office support;
- Administration and *processing* of clients' *personal data* for the purposes of supplying/introducing work- seekers;
- Actively passing and adhering to audit standards as set out by our clients

The Company will only process *personal data* where it has a legal basis for doing so. Where the Company does not have a legal reason for *processing personal data* any *processing* will be a breach of the Data Protection Laws.

Information security

Only those listed in the Appendix are permitted to add, amend or delete personal data from the Company's database(s) ('database' includes paper records or records stored electronically).

All Company staff are responsible for notifying those listed in the Appendix where information is known to be old, inaccurate or out of date or a request for erasure, access, rectification or restriction of *processing* has been received from the individual. Company staff are also responsible for notifying those listed in the Appendix where any request for data portability, objection to *processing* or where *consent* to process has been withdrawn and has been received from the individual.

The incorrect *processing of personal data* e.g. sending an individual's details to the wrong person, allowing unauthorised persons access to personal data, sending information out for purposes for which the individual did not give their *consent*, or not having a lawful reason to process personal data, may give rise to a breach of contract and/or negligence leading to a claim against the Company for damages from an employee, work- seeker or client contact.

A failure to observe the contents of this procedure policy will be treated as a disciplinary offence.

In addition, all Company staff should ensure that adequate security measures are in place to limit the risk of *personal data breaches*. For example:

- Staff should lock their computer screens when they are not in use.
- All devices, whether company or personal devices (including but not limited to computers, mobile phones, other hand-held devices) containing personal data relating to the services of the Company shall be encrypted and password protected.
- Staff should not disclose their passwords to anyone.
- Email should be used with care. Company staff must ensure that emails are sent only to the intended recipient/s. Where Company staff send an email in error then the email must be recalled immediately, and Company staff must inform those listed in the Appendix of the error so that any risk of a *personal data breach* can be limited.
- Personnel files (whether for internal staff or work-seekers) and other personal data should be stored securely to prevent unauthorised access. They should not be removed from their usual place of storage without good reason.
- Personnel files (whether for internal staff or work-seekers) should always be locked away when not in use and when in use should not be left unattended.
- Personal data should only be stored for the periods set out in the Company's data retention

- policy.
- *Processing* includes the destruction or disposal of personal data. Therefore, staff should take care to destroy or dispose of personal data safely and securely. Such material should be shredded or stored as confidential waste awaiting safe destruction.

Rights of the individual

1. The right to be informed

Any individual whose *personal data* is processed by the Company will have the right to be informed about such *processing*. They will have the right to be informed about who, what, where and why the data is processed. This information should be delivered in a privacy notice, in writing and where appropriate electronically. Depending on where the personal data are being collected, an individual may be directed to the Company’s website privacy notice or be given a copy of a privacy notice. This privacy notice should be issued in instances where either:

- a) the Company collects/processes data directly from the individual; or
- b) the Company has not collected/processed the data from the individual directly.

The privacy notice should include the information set out in Table

1 (below). In addition:

- a) Where personal data has been collected **from the individual** the privacy notice will need to be issued at the point the data is collected. Where the Company intends to further process the personal data for a purpose other than that for which the personal data was collected, the Company shall provide the individual, prior to that further *processing*, with information on that other purpose and with any relevant further information in an updated privacy notice.
- b) Where personal data has **not been obtained from the individual**, the Company shall provide the privacy notice within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed. If the personal data are to be used to communicate with the individual, then the privacy notice will be issued at the time of the first communication with the individual. If a disclosure to another recipient is envisaged, then the privacy notice will be issued to the individual at the latest when the personal data are first disclosed.

Company staff will be responsible for issuing privacy notices to individuals whose personal data is processed by the Company in the timeframes and circumstances mentioned above.

Table 1: Privacy information to be given to the individual

	Where the Company collects data from the individual:	Where personal data has not been obtained from the individual:
--	--	--

<ul style="list-style-type: none"> The identity and contact details of the Company and where applicable the controller's representatives and/or data protection officer. 	Yes (Y)	Y
<ul style="list-style-type: none"> The purposes of <i>processing</i> and the legal basis for the <i>processing</i>. 	Y	Y
<ul style="list-style-type: none"> The legitimate interest of the <i>data controller</i> or third party, where applicable. 	Y	Y
<ul style="list-style-type: none"> The categories of personal data. 	No (N)	Y
<ul style="list-style-type: none"> Recipients or categories of recipients of personal data. 	Y	Y
<ul style="list-style-type: none"> Details of transfers to third countries and the safeguards in place. 	Y	Y
<ul style="list-style-type: none"> The retention period of the data or the criteria used to determine the retention period. 	Y	Y
<ul style="list-style-type: none"> The existence of the right to <i>withdraw consent</i> where it has been given and relied upon. 	Y	Y
<ul style="list-style-type: none"> The right to lodge a complaint with the Information Commissioner's Office or any other relevant <i>supervisory authority</i>. 	Y	Y
<ul style="list-style-type: none"> The source the personal data originates from and whether it came from publicly accessible sources. 	N	Y
<ul style="list-style-type: none"> Whether the provision of personal data form part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data. 	Y	N
<ul style="list-style-type: none"> The existence of automated decision-making, including <i>profiling</i> and information about how decisions are made, the significance and the consequences. 	Y	Y

2. The right to access ('subject access request')

Individuals are entitled to obtain access to their personal data on request, free of charge except in certain circumstances.

An individual will be entitled to the following information:

- Confirmation that their personal data is or is not being processed;
- Access to the personal data undergoing *processing*;
- The purposes of the *processing*;

- The categories of personal data concerned;
- The recipients or categories of recipient to whom the personal data have been or will be disclosed, recipients in third countries or international organisations;
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the right to request from the Company rectification or erasure of personal data or restriction of *processing* of personal data concerning the individual or to object to such *processing*;
- The right to lodge a complaint with the ICO or any other relevant *supervisory authority*;
- Where the personal data are not collected from an individual, any available information as to the source of that information;
- The existence of automated decision-making, including *profiling*, based on a public interest or a legitimate interest and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such *processing* for the individual.

If the Company transfers the individual's personal data to a third country or to an international organisation, the individual shall have the right to be informed of the appropriate safeguards in place relating to the transfer.

If the Company processes a large quantity of information concerning the individual making the request, the Company might request that the individual specify the information or *processing* activities to which the request relates to specifically before the information is delivered. If such a request is required by the Company then it shall be delivered promptly to the individual, taking into consideration the timeframes that subject access requests must be completed.

The individual's right to access their information shall not adversely affect the rights and freedoms of others and they will not be able to access the personal data of third parties without the explicit *consent* of that third party or if it is reasonable in all the circumstances to comply with the request without that third party's *consent*, taking into consideration any means to redact the personal data of any third party. Persons listed in the Appendix will decide whether it is appropriate to disclose the information to the individual on a case by case

Note: an individual might not label their subject access request as such. Therefore, Company staff should always consider whether a request is a subject access request even when not called that. If in doubt, refer to the persons listed in the Appendix.

basis. This decision will involve balancing the individual's right of access of their personal data against the third party's rights in respect of their own personal data.

3. The right to rectification

An individual, or another *data controller* acting on an individual's behalf, has the right to obtain from the Company rectification of inaccurate or incomplete personal data concerning him or her. The Company must act on this request without undue delay.

Taking into account the purposes of the *processing*, the individual shall have the right to have

incomplete *personal data* completed, including by means of providing a supplementary statement stating what they would require to be completed.

The Company shall communicate any rectification of *personal data* to each recipient to whom the *personal data* have been disclosed, unless this proves impossible or involves disproportionate effort. The Company shall inform the individual about those recipients if he or she requests it.

Where the Company, acting as a *data processor*, receives information from a *data controller* to rectify an individual's *personal data*, then the Company shall comply with this request unless this proves impossible or involves disproportionate effort.

In circumstances where the Company is unable to comply with the request as it proves impossible or involves disproportionate effort, the Company will document this in a privacy impact assessment or similar.

4. The right to erasure ('the right to be forgotten')

An individual shall have the right to obtain from the Company, acting as *data controller*, the erasure of *personal data* concerning him or her without undue delay. The Company will be obliged to erase the individual's *personal data* without undue delay where one of the following grounds apply:

- The *personal data* are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- An individual withdraws *consent* on which the *processing* is based, and where there is no other legal ground for the *processing*;
- An individual objects to the *processing* (based on either a public interest or a legitimate interest) and there are no overriding legitimate grounds for the *processing*, or an individual objects to the *processing* for direct marketing purposes (including *profiling* related to direct marketing);
- The *personal data* have been unlawfully processed;
- The *personal data* have to be erased for compliance with a legal obligation; or
- The *personal data* have been collected in relation to the offer of information society services to a child.

Where the Company, acting as *data controller*, has made the *personal data* public and is obliged to erase that *personal data*, the Company, taking into account available technology and the cost of implementation, shall take reasonable steps, including technological measures, to inform *data controllers* which are *processing* the *personal data* that an individual has requested the erasure by such controllers of any links to, or copy or replication of, those *personal data*.

The Company will not be obliged to erase information to the extent that *processing* is necessary:

- For exercising the right of freedom of expression and information;
- For compliance with a legal obligation which requires *processing*, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company acting as controller;

- For reasons of public interest in the area of public health;
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or
- For the establishment, exercise or defence of legal claims.

The Company shall communicate any erasure of *personal data* to each recipient to whom the *personal data* have been disclosed, unless this proves impossible or involves disproportionate effort. The Company shall inform the individual about those recipients if an individual request it.

Where the Company, acting as a *data processor*, receives information from a *data controller* to erase an individual's *personal data* the Company shall comply with this request, unless this proves impossible or involves disproportionate effort.

In circumstances where the Company is unable to comply with the request as it proves impossible or involves disproportionate effort, the Company will document this in a privacy impact assessment or similar.

5. The right to restrict processing

An individual will have the right to obtain from the Company, acting as a *data controller*, the restriction of processing his or her personal data where one of the following applies:

- The accuracy of the *personal data* is contested by the individual, for a period enabling the Company to verify the accuracy of the *personal data*;
- The *processing* is unlawful and the individual opposes the erasure of the *personal data* and requests the restriction of their use instead;
- The Company no longer needs the *personal data* for the purposes of the *processing*, but they are required by an individual for the establishment, exercise or defence of legal claims;
- The individual has objected to *processing* (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of the Company override those of the individual.

Where *processing* has been restricted, such *personal data* shall, with the exception of storage, only be processed with the individual's *consent* or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.

Where an individual who has successfully asked for their *personal data* to be restricted, then the Company will inform the individual before such a restriction is lifted.

The Company shall communicate any restriction of *processing* to each recipient to whom the *personal data* have been disclosed, unless this proves impossible or involves disproportionate effort. The Company shall inform the individual about those recipients if he or she requests it.

Where the Company, acting as a *data processor*, receives information from a *data controller* to restrict *processing* an individual's *personal data*, the Company shall comply with this request, unless this proves impossible or involves disproportionate effort.

In circumstances where the Company is unable to comply with the request as it proves impossible

or involves disproportionate effort, the Company will document this in a privacy impact assessment or similar.

6. The right to data portability

An individual has the right to receive any *personal data* concerning him or her, which he or she has provided to the Company, in a structured, commonly used and machine-readable format and have the right to transmit those data to another *data controller* where:

- The *processing* is based on the individual's *consent* or a contract; and
- The *processing* is carried out by automated means.

Company staff will advise those listed in the Appendix when they receive a request to port data. Those listed in the Appendix will be responsible for identifying if the above circumstances are satisfied for the purposes of porting the data to the individual and/or another *data controller*. For the avoidance of doubt, there is no obligation to port *personal data* that is not kept by automated means by the Company.

7. The right to object to processing

An individual, has the right to object to their *personal data* being processed or profiled based on a public interest or a legitimate interest.

Where the Company receives an objection to *processing* or *profiling* on the above, those listed in the Appendix will ensure that the *processing* and/or *profiling* ceases unless such persons can establish compelling grounds to continue to process the *personal data*. If this is the case those persons listed in the Appendix will document this in a privacy impact assessment or similar.

8. Automated decision-making processes

An individual has the right not to be subjected to an automated decision-making process, including *profiling*, that produces a legal effect or a similarly significant effect on the individual.

However, it is possible to subject an individual to automated decision making processes, including *profiling*, where:

- a) It is necessary for entering into or performance of a contract between the employer and the individual;
- b) It is authorised by law; or
- c) The individual has given their explicit *consent*.

Where a) and c) apply the Company will ensure that suitable measures are in place to safeguard the individual's rights and freedoms and legitimate interests, under both Data Protection Laws and the Human Rights Act 1998, before this type of *processing* occurs for *personal data*.

Where a) to c) apply the Company will only process *sensitive personal data* where the Company has received either the explicit *consent* to do so or there is a substantial public interest to do so. Again, the Company will ensure that suitable measures are in place to safeguard the individual's rights and freedoms and legitimate interests, under both Data Protection Laws and the Human Rights Act 1998, before this type of *processing* occurs for *sensitive personal data*.

The safeguarding measures include:

- Conducting a risk assessment as to what risks are posed to the individual's rights and freedoms;
- Ensuring where the automated decision-making process is necessary for entering into or performance of a contract, that this is documented clearly by the Company;
- Ensuring where explicit *consent* is given this is documented clearly by the Company – and;
- Include any other measures that your Company will implement.

The persons listed in the Appendix will be responsible for implementing the above safeguarding measures. Company staff will be responsible for informing those persons listed in Appendix immediately in order to implement the above safeguards.

9. The right to withdraw consent

Where the Company relies on an individual's *consent* to process their *personal data* then the Company will advise the individual that they have the right to withdraw his or her *consent* at any time.

Any Company staff who receives a request from an individual to withdraw their *consent* to *processing* their data will inform the persons listed in **the** Appendix to process the individual's request further.

10. Timing and information to be provided to the individual

The Company shall provide information on action taken or not taken with regards to the individual data protection rights, set out in paragraphs 1 to 9 inclusive, without undue delay and in any event **within one month of receipt of the request**. Where the Company does act, then it may, where necessary, extend this period by a further two months, taking into account the complexity and number of the requests. Those persons listed in the Appendix shall inform an individual of any extension within one month of receipt of the request, together with the reasons for the delay. Where the Company does not take action on the request of the individual then those persons listed in the Appendix will inform him or her on the possibility of lodging a complaint with the ICO and seeking a judicial remedy.

11. Charges

Where requests from an individual are manifestly unfounded or excessive, in particular because of their repetitive character, the Company may either:

- Charge a reasonable fee considering the administrative costs of providing the information or communication or taking the action requested; or
- Refuse to act on the request.

The Company must demonstrate whether the request is manifestly unfounded or excessive. Those listed in the Appendix will be responsible for demonstrating this.

Where the individual makes the request by electronic means the Company shall provide the information in a commonly used electronic form, unless otherwise requested by the individual.

Personal data breaches

Those listed in the Appendix will take measures to establish whether a *personal data breach* has occurred. Those persons will:

- Conduct a risk assessment as to what level of risk the *personal data breach* poses/has occurred;
- Conduct any relevant interviews or investigations of the Company's practices and/or Company staff to assess how the *personal data breach* occurred;
- Implement measures and take steps to limit, contain and recover the breach;
- Include any other measures that your Company will implement.

Unless the *personal data breach* is unlikely to result in a risk to the rights and freedoms of an individual, then those listed in the Appendix will be responsible for alerting the ICO of any *personal data breach* without undue delay, but no later than 72 hours after having become aware of the Company's *personal data breach*. Where it is not possible to inform the ICO in this time those listed in the Appendix will be responsible for explaining to the ICO the reasons for the delay.

If the *personal data breach* happens outside the UK, then those listed in the Appendix will be responsible for alerting the relevant *supervisory authority* in the effected jurisdiction.

If those listed in the Appendix are not able to provide the ICO/other relevant *supervisory authority* with all the relevant information related to the *personal data breach* then those persons shall provide the information in phases without undue further delay.

Those listed in the Appendix will be responsible for documenting any personal data breaches, including:

- The facts relating to the *personal data breach* – including any investigations undertaken or statements taken from the Company's staff;
- The effects of the *personal data breach*; and
- The remedial action taken.

Personal data breaches where the Company is the data processor:

Those listed in the Appendix will be responsible for alerting the relevant *data controller* as to the

personal data breach that has been identified as soon as they are aware of the breach, having particular regard to any contractual obligations the Company has with the *data controller*.

Communicating personal data breaches to individuals

Where a *personal data breach* has been identified, which results in a high risk to the rights and freedoms of individuals, those listed in the Appendix will be responsible for informing those individuals effected by the *personal data breach* without undue delay.

For the avoidance of doubt there will be no need to inform individuals of a *personal data breach* where:

- The Company has implemented appropriate technical and organisational protection measures to use the *personal data* affected by the breach, in particular to make the *personal data* unintelligible to any person who is not authorised to access it, such as encryption.
- The Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialise.
- It would involve disproportionate effort to tell all affected individuals. Instead, those listed in the Appendix shall, on behalf of the Company, make a public communication or similar measure to tell all affected individuals.

Complaints

Where Company staff receive a complaint from an individual about the use of his or her *personal data* then they should bring this to the immediate attention of those listed in the Appendix.

Appendix

List of those responsible people for the following:

- adding, amending or deleting *personal data*; **Yasmin Mandil – Head of Compliance**
- responding to subject access requests/requests for rectification, erasure, restriction data portability, objection, automated decision-making processes and *profiling* and withdrawal of *consent*; **Barry Pactor - CEO**
- reporting data breaches/dealing with complaints; and details of the Data Protection Officer where applicable. **Yasmin Mandil – Head of Compliance**