Privacy Notice

Company Name:	Premises Recruitment Limited Registered in England and Wales No: 4216304
Company Contact details:	Abbey Stephenson Suite 3, 258 High Road, Loughton, Essex, IG10 1RB Tel: 0208 502 0111 Email: gdpr@premisesrecruitment.com
Topic:	Data Protection
Date:	25th May 2018
Version:	1.0

Premises Recruitment Limited is a recruitment business which provides work-finding services to its clients and work-seekers. Premises must process personal data (including sensitive personal data) so that it can provide these services – in doing so, Premises acts as a data controller.

You may give your personal details to Premises directly, such as on an application or registration form or via our website, or we may collect them from another source such as a jobs board. Premises must have a legal basis for processing your personal data. For the purposes of providing you with work-finding services and/or information relating to roles relevant to you we will only use your personal data in accordance with the terms of the following statement. At all times we will comply with current data protection laws.

Contents

1. Collection And Use Of Personal Data

- **a. The purpose of Premises processing your data and the legal basis for doing so**

Premises will collect your personal data (which may include sensitive personal data) and will process your personal data for the purposes of providing you with work-finding services.

This includes for example, contacting you about job opportunities, assessing your suitability for those opportunities, updating our databases, putting you forward for job opportunities, arranging payments to you and developing and managing our services and relationship with you and our clients.

If you have opted-in we may also send you marketing information and news via email/ text. You can opt-out from receiving these at any time by clicking "unsubscribe" when you receive these communications from us.

In some cases we may be required to use your data for the purpose of investigating, reporting and detecting crime and also to comply with laws that apply to us. We may also use your information during the course of internal audits to demonstrate our compliance with certain industry standards.

We must have a legal basis to process your personal data. The legal bases we rely upon to offer these services to you are:

- Your consent
- Where we have a legitimate interest
- To comply with a legal obligation that we have
- To fulfil a contractual obligation that we have with you

- **b. Legitimate interest**

This is where Premises has a legitimate reason to process your data provided it is reasonable and does not go against what you would reasonably expect from us. Where Premises has relied on a legitimate interest to process your personal data our legitimate interests are as follows:

- Managing our database and keeping work-seeker records up to date;
- Providing work-finding services to you and our clients;
- Contacting you to seek your consent where we need it;
- Giving you information about similar products or services that you have used from us recently;

- **c. Statutory/contractual requirement**

The Company has certain legal and contractual requirements to collect personal data (e.g. to comply with the Conduct of Employment Agencies and Employment Businesses Regulations 2003, immigration and tax legislation, and in some circumstances safeguarding requirements.) Our clients may also require this personal data, and/or we may need your data to enter into a contract with you. If you do not give us personal data we need to collect we may not be able to continue to provide work-finding services to you, or process wage payments for any undertaking of temporary assignment.

- **d. Recipients of data**

Premises will process your personal data and/or sensitive personal data with the following recipients.

- Our clients (whom we may introduce or supply you to)
- Former employers whom we may seek references from
- Our trusted recruitment CRM software provider
- Payroll service providers who manage payroll on our behalf or other payment intermediaries whom we may introduce you to

2. Information to be provided when data is not collected directly from the data subject

Categories of data: We have collected the following personal data on you:

Personal data:

- Name, address, mobile No., email
- National insurance No.
- Nationality (through right to work check)
- CV/Employment History
- Other Work Related Information

Sensitive personal data:

- Health information including whether you have a disability
- Criminal conviction

Source of the personal data: We may obtain your personal data from the following sources (please note that this list is not exhaustive):

- Jobs boards (TotalJobs, CareerStructure, CV Library)
- LinkedIn
- A former employer
- A referee whose details you previously provided to us
- Industry leads service (Glenigans)

Where you are a Candidate and we have obtained your personal data from a third party such as an online job board, it is our policy to advise you of the source when we first communicate with you.

3. Overseas Transfers

Premises will not transfer the information you provide to us to countries outside the European Economic Area ('EEA') for the purposes of providing you with work-finding services. The EEA comprises the EU member states plus Norway, Iceland and Liechtenstein.

4. Data Retention

Premises will retain your personal data only for as long as is necessary for the purpose we collect it. Different laws may also require us to keep different data for different periods of time.

The Conduct of Employment Agencies and Employment Businesses Regulations 2003, require us to keep work-seeker records for at least one year from (a) the date of their creation or (b) after the date on which we last provide you with work-finding services.

We must also keep your payroll records, holiday pay, sick pay and pensions auto-enrolment records for as long as is legally required by HMRC and associated national minimum wage, social security and tax legislation. This is currently 3 to 6 years.

Where Premises has obtained your consent to process your personal and/or sensitive personal data, we will do so in line with our retention policy (which is available on request).

Upon expiry of that period Premises will seek further consent from you. Upon seeking further consent if further consent is not granted Premises will cease to process your personal data and sensitive personal data.

5. Your Rights

Please be aware that you have the following data protection rights:

- The right to be informed about the personal data Premises processes on you;
- The right of access to the personal data Premises processes on you;
- The right to rectification of your personal data;
- The right to erasure of your personal data in certain circumstances;
- The right to restrict processing of your personal data;
- The right to data portability in certain circumstances;
- The right to object to the processing of your personal data that was based on a public or legitimate interest;
- The right not to be subjected to automated decision making and profiling; and
- The right to withdraw consent at any time.

Where you have consented to Premises processing your personal data and/or sensitive personal data you have the right to withdraw that consent at any time by contacting:

Abbey Stephenson

Suite 3, 258 High Road, Loughton, Essex, IG10 1RB

Tel: 0208 502 0111 Email: gdpr@premisesrecruitment.com

There may be circumstances where Premises will still need to process your data for legal or official reasons. We will inform you if this is the case. Where this is the case, we will restrict the data to only what is necessary for the purpose of meeting those specific reasons.

If you believe that any of your data that Premises processes is incorrect or incomplete, please contact us using the details above and we will take reasonable steps to check its accuracy and correct it where necessary.

You can also contact us using the above details if you want us to restrict the type or amount of data we process for you, access your personal data or exercise any of the other rights listed above.

6. Cookies

We may obtain data about you from cookies. These are small text files that are placed on your computer by websites that you visit. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site. Cookies also enable us to deliver more personalised content.

The table below explains the cookies we use and why.

Cookie	Name	Purpose	More information

Most web browsers allow some control of most cookies through the browser settings. To find out more about cookies, please refer to our Cookie policy. Please note that in

a few cases some of our website features may not function if you remove cookies from your browser.

7. Log Files

We use IP addresses to analyse trends, administer the site, track users' movements, and to gather broad demographic information for aggregate use. IP addresses are not linked to personally identifiable information.

8. Links To External Websites

Our website may contain links to other external websites. Please be aware that we are not responsible for the privacy practices of such other sites. When you leave our site we encourage you to read the privacy statements of each and every website that collects personally identifiable information. This privacy statement applies solely to information collected by the our website.

9. Sale of Business

If our business is sold or integrated with another business your details may be disclosed to our advisers and any prospective purchasers and their advisers and will be passed on to the new owners of the business.

10. Data Security

The Company takes every precaution to protect our users' information. We utilise a fully hosted secure recruitment system with high level security measures in place in relation to the personal data processed, including firewall, browser certification technology, limited access rights, and password protection.

Only employees who need the information to perform a specific job (for example, consultants, our accounts clerk or a marketing assistant) are granted access to your information.

Premises uses all reasonable efforts to safeguard your personal information. However, you should be aware that the use of email/ the Internet is not entirely secure and for this reason we cannot guarantee the security or integrity of any personal information which is transferred from you or to you via email/ the Internet.

If you share a device with others we recommend that you do not select the "remember my details" function when that option is offered.

If you have any questions about the security at our website, you can email gdpr@premisesrecruitment.com

11. Changes To This Privacy Statement

We will update this privacy statement from time to time. We will post any changes on the statement with revision dates. If we make any material changes, we will notify you.

12. Complaints Or Queries

If you wish to complain about this privacy notice or any of the procedures set out in it please contact:

Abbey Stephenson – Director, undertaking duties of Data Protection Officer

Suite 3, 258 High Road, Loughton, Essex, IG10 1RB

Tel: 0208 502 0111 Email: gdpr@premisesrecruitment.com

You also have the right to raise concerns with Information Commissioner's Office on 0303 123 1113 or at https://ico.org.uk/concerns/, or any other relevant supervisory authority should your personal data be processed outside of the UK, if you believe that your data protection rights have not been adhered to.

Data Protection Policy

Company Name:	Premises Recruitment Ltd ('the Company')
Date:	25th May 2018
Version:	1.0

Contents

- Complaints

Appendix

Annex – legal bases for processing personal data

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 (known as 'data subjects') 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 how the Company implements the Data Protection Laws.

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. [Note 1]

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

'*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 has registered with the ICO and its registration number is ZA343032.

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

- Staff administration;
- Advertising, marketing and public relations;
- 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;

1. The data protection principles

The Data Protection Laws require the Company acting as either *data controller* or *data processor* to process data in accordance with the principles of data protection. These require that *personal data* is:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and kept up to date; every reasonable step must be taken to ensure that *personal data* that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept for no longer than is necessary for the purposes for which the *personal data* are processed;
6. Processed in a manner that ensures appropriate security of the *personal data*, including protection against unauthorised or unlawful *processing* and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and that
7. The *data controller* shall be responsible for, and be able to demonstrate, compliance with the principles.

2. Legal bases for processing

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

The Company will review the *personal data* it holds on a regular basis to ensure it is being lawfully processed and it is accurate, relevant and up to date and those people listed in the Appendix shall be responsible for doing this.

Before transferring *personal data* to any third party (such as past, current or prospective employers, suppliers, customers and clients, intermediaries such as umbrella companies, persons making an enquiry or complaint and any other third party (such as software solutions providers and back office support)), the Company will establish that it has a legal reason for making the transfer.

3. Privacy by design and by default

The Company has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all *processing* activities. This includes implementing measures such as data minimisation i.e. not keeping data longer than necessary, anonymization (when/if appropriate) and operating a secure CRM processing system and API (Automated Programmable Interface) accessed through the Company's Website portal.

Rights Of The Individual

The Company shall provide any information relating to data *processing* to an individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. The Company may provide this information orally if requested to do so by the individual.

1. Privacy notices

Where the Company collects *personal data* from the individual, the Company will give the individual a privacy notice at the time when it first obtains the *personal data*.

Where the Company collects *personal data* other than from the individual directly, it will give the individual a privacy notice within a reasonable period after obtaining the *personal data*, but at the latest within one month. If the Company intends to disclose the *personal data* to a third party then the privacy notice will be issued when the *personal data* are first disclosed (if not issued sooner).

Where the Company intends to further process the *personal data* for a purpose other than that for which the data was initially collected, the Company will give the individual information on that other purpose and any relevant further information before it does the further *processing*.

2. Subject access requests

The individual is entitled to access their *personal data* on request from the *data controller*.

3. Rectification

The individual or another *data controller* at the individual's request, has the right to ask the Company to rectify any inaccurate or incomplete *personal data* concerning an individual.

If the Company has given the personal data to any third parties it will tell those third parties that it has received a request to rectify the *personal data* unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold - however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

4. Erasure

The individual or another *data controller* at the individual's request, has the right to ask the Company to erase an individual's *personal data.*

If the Company receives a request to erase it will ask the individual if s/he wants his *personal data* to be removed entirely or whether s/he is happy for his or her details to be kept on a list of individuals who do not want to be contacted in the future (for a specified period or otherwise). The Company cannot keep a record of

individuals whose data it has erased so the individual may be contacted again by the Company should the Company come into possession of the individual's *personal data* at a later date.

If the Company has made the data public, it shall take reasonable steps to inform other *data controllers* and *data processors processing* the *personal data* to erase the *personal data*, taking into account available technology and the cost of implementation.

If the Company has given the *personal data* to any third parties it will tell those third parties that it has received a request to erase the *personal data*, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold - however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

5. Restriction of *processing*

The individual or a *data controller* at the individual's request,has the right to ask the Company to restrict its *processing* of an individual's *personal data* where:

- The individual challenges the accuracy of the *personal data*;
- The *processing* is unlawful and the individual opposes its erasure;
- The Company no longer needs the *personal data* for the purposes of the *processing*, but the *personal data* is required for the establishment, exercise or defence of legal claims; or
- 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.

If the Company has given the *personal data* to any third parties it will tell those third parties that it has received a request to restrict the *personal data*, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold - however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

6. Data portability

The individual shall have the right to receive *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* in circumstances where:

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

Where feasible, the Company will send the *personal data* to a named third party on the individual's request.

7. Object to *processing*

The individual has the right to object to their *personal data* being processed based on a public interest or a legitimate interest. The individual will also be able to object to the *profiling* of their data based on a public interest or a legitimate interest.

The Company shall cease *processing* unless it has compelling legitimate grounds to continue to process the *personal data* which override the individual's interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

The individual has the right to object to their *personal data* for direct marketing.

8. Enforcement of rights

All requests regarding individual rights should be sent to the person whose details are listed in the Appendix.

The Company shall act upon any subject access request, or any request relating to rectification, erasure, restriction, data portability or objection or automated decision making processes or profiling within one month of receipt of the request. The Company may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

Where the Company considers that a request under this section is manifestly unfounded or excessive due to the request's repetitive nature the Company may either refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved.

9. Automated decision making

The Company will not subject individuals to decisions based on automated *processing* that produce a legal effect or a similarly significant effect on the individual, except where the automated decision:

- Is necessary for the entering into or performance of a contract between the *data controller* and the individual;
- Is authorised by law; or
- The individual has given their explicit *consent*.

The Company will not carry out any automated decision-making or *profiling* using the *personal data* of a child.

Reporting *Personal Data* Breaches

All data breaches should be referred to the persons whose details are listed in the Appendix.

1. ***Personal data breaches*** **where the Company is the** ***data controller*****:**

Where the Company establishes that a *personal data breach* has taken place, the Company will take steps to contain and recover the breach. Where a *personal data breach* is likely to result in a risk to the rights and freedoms of any individual the Company will notify the ICO.

Where the *personal data breach* happens outside the UK, the Company shall alert the relevant *supervisory authority* for data breaches in the effected jurisdiction.

2. ***Personal data breaches*** **where the Company is the** ***data processor*****:**

The Company will alert the relevant *data controller* as to the *personal data breach* as soon as they are aware of the breach.

3. **Communicating** ***personal data breaches*** **to individuals**

Where the Company has identified a *personal data breach* resulting in a high risk to the rights and freedoms of any individual, the Company shall tell all affected individuals without undue delay.

The Company will not be required to tell individuals about the *personal data breach* where:

- The Company has implemented appropriate technical and organisational protection measures to 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, the Company shall make a public communication or similar measure to tell all affected individuals.

All individuals have the following rights under the Human Rights Act 1998 (HRA) and in dealing with *personal data* these should be respected at all times:

- Right to respect for private and family life (Article 8).
- Freedom of thought, belief and religion (Article 9).
- Freedom of expression (Article 10).
- Freedom of assembly and association (Article 11).
- Protection from discrimination in respect of rights and freedoms under the HRA (Article 14).

Complaints

If you have a complaint or suggestion about the Company's handling of *personal data* then please contact:

Abbey Stephenson - Premises Recruitment Ltd - Data Protection Officer

Email: gdpr@premisesrecruitment.com

Tel: 020 8502 0111

Alternatively you can contact the ICO directly on 0303 123 1113 or at https://ico.org.uk/global/contact-us/email/

Appendix

a) **The lawfulness of *processing* conditions for *personal data* are:**

- *Consent* of the individual for one or more specific purposes.
- *Processing* is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual to enter into a contract.
- *Processing* is necessary for compliance with a legal obligation that the controller is subject to.
- *Processing* is necessary to protect the vital interests of the individual or another person.
- *Processing* is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the *data controller*.
- *Processing* is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of the individual which require protection of *personal data*, in particular where the individual is a child.

b) **The lawfulness of *processing* conditions for *sensitive personal data* are:**

1. Explicit *consent* of the individual for one or more specified purposes, unless reliance on *consent* is prohibited by EU or Member State law.
2. *Processing* is necessary for carrying out data controller's obligations under employment, social security or social protection law, or a collective agreement, providing for appropriate safeguards for the fundamental rights and interests of the individual.
3. *Processing* is necessary to protect the vital nterests of the individual or another individual where the individual is physically or legally incapable of giving *consent*.
4. In the course of its legitimate activities*, processing* is carried out with appropriate safeguards by a foundation, association or any other not-for-profit body, with a political, philosophical, religious or trade union aim and on condition that the *processing* relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without the *consent* of the individual.
5. *Processing* relates to *personal data* which are manifestly made public by the individual.
6. *Processing* is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
7. *Processing* is necessary for reasons of substantial public interest on the basis of EU or Member State law which shall be proportionate to the aim pursued, respects the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the individual.
8. *Processing* is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, 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 EU or Member State law or a contract with a health professional and subject to the necessary conditions and safeguards.

9. *Processing* is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of EU or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the individual, in particular professional secrecy.
10. *Processing* is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard fundamental rights and interests of the individual.