JIK Software Ltd

Data Protection Policy

Version	Release 1
Date	April 24 2018
Owner	Peter Knowles Chief Executive
Author	Ben Darlington CTIDO

1. Introduction

1.1 Overview

Respecting and protecting the Privacy of our clients and users is baked into the heart of everything we do and reflected in our brand strapline:

Your Success matters. ***Your Privacy matters.*** *You matter.*

The new GDPR Regulations, which come into force in May 2018, may be changing the legal context but we have generally always exceeded legislative and regulatory requirements when it comes to collecting, protecting and processing the Personal Data of our users. The importance we attach to the privacy of our users and protecting the data they share with us means that will remain the case.

Our Policy is this area reflects those values and behaviours.

1.2 Purpose, Structure, Scope and intended Readership of this policy document

The purpose of this Policy document is to provide our staff, clients, users and stakeholders with a clear definition of exactly what our principles are in respect of the collection, use, retention, transfer, disclosure and destruction of Personal Data and how those principles are and must be reflected in our systems and working practices.

The Document defines the seven, Data Protection principles to which we adhere and then provides practical, detailed examples or instructions for how each of those principles should be effected in the way we build our systems and deliver our services.

The Scope of this document is limited to that purpose: there is no specific discussion of any the services we provide or the business model associated with any service.

This document MUST be read by all JIK staff and management and may be read by any other individual interested in understanding our policy.

1.3 Further information

Any requests for further information or to notify us of any concerns or questions you may have about our collection, use, retention, transfer, disclosure or destruction of Personal Data please contact:

support@jiksoftware.ltd.uk

2. Our Data Protection Policy

2.1 Governance

Our Chief Executive is directly responsible for ensuring that we handle the personal data of our users with integrity and care; that we should be fully compliant with not only the letter but also the spirit of any relevant legislation is our floor, not our ceiling.

Our Chief Executive also acts as a point of contact for, notifying and cooperating with Data Protection Authorities (DPA's) and ensures that a Data Protection Impact Assessment (DPIA) is conducted for any new processes or services which might in any way touch user data.

Any staff members who have concerns about or who identify any deficiencies in the way we are collecting, storing or processing user data are actively asked to report their concerns directly to the Chief Executive, who is responsible for ensuring that the reports are acted on and that any necessary remedial action is taken.

2.2 Our Data Protection Principles

We have adopted the following, broad principles to govern our collection, use, retention, transfer, disclosure and destruction of Personal Data:

Principle 1: Lawfulness, Fairness and Transparency

Whenever we process Personal Data, we will do so lawfully, fairly and in a transparent manner in relation to the Data Subject (the individual whose data is being processed).

This means that we will always tell the Data Subject what Processing will occur in a way which is understandable (transparency), we will always seek Consent to the processing when Consent is required (lawfully) and the Processing will always match the description given to the Data Subject (fairness) and/or for one of the purposes specified in the applicable Data Protection regulations (lawfulness again).

Principle 2: Purpose Limitation

We will only collect Personal Data for specified, explicit and legitimate purposes and not process the data in a manner that is incompatible with those purposes.

This means we will specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation

We will only store Personal Data which is necessary in relation to the purposes for which they are processed.

Principle 4: Accuracy

We will make efforts to keep Personal Data accurate and up to date.

This means we will have in place processes for identifying Personal Data which might be out-of-date, incorrect or redundant and contact the Data Subject to verify the Personal Data and rectify, as required.

Principle 5: Storage Limitation

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed.

This means that wherever and whenever possible, we will store Personal Data in a way that limits or prevents identification of the Data Subject.

Principle 6: Integrity & Confidentiality

We will process Personal Data 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.

This means we will use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained.

Principle 7: Accountability

We will be able to demonstrate compliance with the six Data Protection Principles (outlined above).

This means that we will review our collection, use, retention, transfer, disclosure and destruction of Personal Data on a regular basis or as required by our Chief Executive.

2.3 Our Data Collection Practices

Data Sources

Personal Data will only be sourced directly from the Data Subject and NOT from 3rd parties unless the collection must be carried out under emergency circumstances in order to:

- Protect the vital interests of the Data Subject
- Prevent serious loss or injury to another person
- Respond to requests from law enforcement agencies.

Data Subject Consent

We will obtain Personal Data only by lawful and fair means and with the knowledge and Consent of the Data Subject – the individual to which the Personal Data relates.

Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, we are committed to seeking such Consent.

In all cases when proposing to collect or process Personal Data or process Personal Data for a purpose other than that for which consent was previously given, we will:

- Determine what disclosures should be made in order to obtain valid Consent.

- Ensure the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.

- Ensure the Consent can be freely given (i.e. not make access to or use of a service we provide – such as applying for a job via one of our web sites - conditional on giving Consent, unless required by the specific service being accessed).

- Document the date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consents given.

- Provide a simple and straightforward method for a Data Subject to withdraw their Consent at any time.

Data Subject Notification

We will provide Data Subjects, when required by applicable law, contract, or when it is reasonably appropriate to do so, with information as to the purpose of the Processing of their Personal Data.

When the Data Subject is asked to give Consent to the Processing of Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures will be made, unless one of the following apply:

- The Data Subject already has the information
- A legal exemption applies to the requirements for disclosure and/or Consent.

The disclosures will usually be made on the website which the customer (advertiser or job seeker) is using but they may be given orally (usually over the telephone) or via email.

If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Chief Executive. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

External Privacy Notices

Each of our job board websites will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law.

All Privacy and Cookie Notices must be approved by the Chief Executive prior to publication on any of our websites.

2.4 Our Data Usage Practices

Data Processing

We use the Personal Data of our users (job seekers) to provide them with a better job search, job alert, job application and CV analysis service and to make it possible for employers to identify job seekers with skills or experience which are relevant to a vacancy they may be looking to fill.

We always consider the use of Personal Data from the perspective of the Data Subject – will it be within their expectations: would an

average person of average intelligence, education and background (ie: not a highly technical person) expect us to do what we do?

For example, it would clearly be within a User's expectations that their CV will be provided to an employer when they apply for a job. However, it would not be within their reasonable expectations that their CV would be provided to other organisations to which they had not applied unless their consent had been explicitly given for us to do so.

As a minimum, we will always Process Personal Data in accordance with all applicable laws and will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has truly given Consent to the Processing of their Personal Data for one or more specific purposes.
- Processing is necessary for us to able to deliver a service and the Data Subject using the service can be expected to have clearly understood that (in which case consent will be implied).
- Processing is necessary for compliance with a legal obligation to which we are subject.
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural 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 us.
- Processing is necessary for the purposes of our legitimate interests except where such interests are over-ridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child.

Children's Data

Children are unable to Consent to the Processing of Personal Data.

Consent must be sought from the person who holds parental responsibility over the child.

However, we can only identify a Data Subject as a child if the Data Subject chooses to provide us with data which allows us to reliably confirm their age. We have to strike the right balance between identifying when one of our users is a child with the need to provide adult users – who form the vast majority of our user base – with a good service.

The express permission of the Chief Executive is required before any Processing of a child's Personal Data may commence, even if valid, parental consent has been given or if Processing is lawful under other grounds.

Data Quality

We are reliant on the Data Subject to provide Personal Data which is complete and accurate and is updated to reflect the current situation of the Data Subject.

We will send regular emails to our users (when we have their permission to do) providing them with an overview of the analysis of their Personal Data (generally their CV and a history of their job viewing and job application history).

The same email will also provide links and instructions which explain how to change, add to or delete the Personal Data we hold or change consents previously given.

Profiling & Automated Decision-Making

We do not and will not seek to classify users against any pre-defined types, categories or 'profiles'.

When the Data Subject has given their consent, we do analyse the Personal Data we have to be able to match a Data Subject (a job seeker) to appropriate job vacancies.

We do also allow employers and recruiters to 'search by template', loading up an ideal description of a candidate and then searching for Data Subjects according to how well they match this 'ideal template'.

We will only include the Personal Data of a Data Subject in this matching process when the Data Subject has given their fully informed consent.

In both cases, there is no 'automated decision making' involved or, if there is, only in so far as a search engine makes automated decisions when ranking search results.

Digital Marketing

When a Data Subject has an account with us, there are some emails and communications which we need to be able to send in order to deliver our service (such as password reset emails or emails confirming job applications made).

We do not regard these as marketing emails and we make it clear to a Data Subject that when have an account with us, they are giving us permission to store their email address, their CV (when uploaded) and send a minimum set of emails. We provide a clear and easy way for a user to close their account and delete all Personal Data held.

There are other emails we may want to send to encourage a Data Subject to make greater use of our services. We will not send such promotional or direct marketing material to a Data Subject (a private individual who has given us their Personal Data) through digital channels such as mobile phones, email and the Internet, without first obtaining their Consent.

When we do have consent, the Data Subject will still be informed with every communication and email that they can withdraw their consent, with links to guidance on how to do so provided in the communication.

Where digital marketing is carried out in a 'business to business' context, there may be no legal requirement to obtain consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out but we nevertheless still seek to obtain consent, typically be

telephone, before any email address is entered into our systems for marketing purposes.

Data Retention

To ensure fair Processing, Personal Data will not be retained by us for longer than necessary in relation to the purposes for which it was originally collected.

The length of time for which we will retain Personal Data is set out in our 'Personal Data Retention Schedule'.

Data Protection

All Personal Data is and will be stored on our own, physical servers located in secure, UK data centres.

We do make use of virtual servers running in cloud environments located in the UK but when data is stored on these servers, any data which could identify the individual is removed.

Data Subject Requests

All Data Subjects who have given their consent will be regularly emailed with information concerning the Personal Data we hold about them and asked to check that the data is accurate, correcting it if not.

We also provide links to an on-line service allowing a Data Subject to revoke or renew any consents given or delete their account. There is also an email address given to which Data Subjects can email their Consent or Account management requests.

No administration fee will be charged for considering and/or complying with any requests received from Data Subjects unless the request is deemed to be unnecessary or excessive in nature.

Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

Data Protection Training

All Employees that have access to Personal Data will have their responsibilities under this policy outlined to them as part of their staff induction training.

In addition, we will provide regular Data Protection training and procedural guidance for staff.

Data Transfers

We will not transfer Personal Data to Third Party Data Controllers unless the Data Subject has given their explicit consent to such a transfer.

We will only transfer Personal Data to Third Party Data Processors when we are assured that the information will be Processed legitimately and protected appropriately by the Data Processors.

We will require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with our instructions. In addition, we will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches.

2.5 Complaints Handling

Data Subjects with a complaint about the Processing of their Personal Data, should put forward the matter in writing to our Chief Executive.

An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. We will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation with the Data Subject, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Information Commissioners Office.

2.6 Breach Reporting

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the Chief Executive providing a description of what occurred.

The Chief Executive will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, we will follow the relevant authorised procedure based on the criticality and quantity of the Personal Data involved.

DOCUMENT ENDS.