Privacy Policy – HR Related Data

Introduction

Purpose

Bango is committed to being transparent about how we collect and use your personal data, and to meeting our data protection obligations. This policy sets out our commitment to data protection, and your individual rights and obligations in relation to personal data.

This policy applies to HR related personal data, that is, the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees. This policy does not apply to the personal data of clients or other personal data processed for business purposes.

We have appointed Rachel Greenhalgh as our data protection officer. Her role is to inform and advise
us on our data protection obligations. Rachel can be contacted at dataprivacy@bango.com

Questions about this policy, or requests for further information, should be directed to Rachel.

Definitions

"Personal data" is any information relating to an identified or identifiable natural person ("data subject"). A person is identifiable if he or she "can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number (e.g. National Insurance number, bank account number, passport number), location data (e.g. home address), an online identifier (e.g. email address), or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity" of that person.

"Processing" is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

We process your HR-related personal data in accordance with the following data protection principles:

- We process your personal data lawfully, fairly and in a transparent manner.
- We collect your personal data only for specified, explicit and legitimate purposes.
- We process your personal data only where it is adequate, relevant and limited to what is necessary
- for the purposes of processing.

- We keep accurate personal data and take all reasonable steps to ensure that inaccurate personal
- data is rectified or deleted without delay.
- We keep your personal data only for the period necessary for processing.
- We adopt appropriate measures to make sure that your personal data is secure, and protected
- against unauthorised or unlawful processing, and accidental loss, destruction or damage.

We advise you of the reasons for processing your personal data, how we use such data and the legal basis for processing in our employee and job applicant privacy notices. We will not process your personal data for other reasons. Where we rely on our legitimate interests as the basis for processing your data, we will carry out an assessment to ensure that those interests are not overridden by your rights and freedoms.

Where we process special categories of your personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with our data protection obligations.

We expect you to update your HR-related personal data promptly in PeopleHR if your information has changed or is inaccurate. If you have any difficulty in doing this you should advise HR immediately.

Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in your personnel file (in hard copy or electronic format, or both), and on our HR information systems. The periods for which we hold HR-related personal data are contained in our employee and job applicant privacy notices.

We keep a record of our processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Individual rights

As a data subject, you have a number of rights in relation to your personal data.

Subject access requests

You have the right to make a subject access request. If you make a subject access request, we will tell you:

- whether or not your data is processed and if so why, the categories of personal data concerned and
- the source of the data if it is not collected from you;
- to whom your data is or may be disclosed, including to recipients located outside the European
- Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long your personal data is stored (or how that period is decided);
- your rights to rectification or erasure of data, or to restrict or object to processing;
- your right to complain to the Information Commissioner if you think we have failed to comply with your data protection rights; and
- whether or not we carry out automated decision-making and the logic involved in any such decision making.

We will also provide you with a copy of your personal data undergoing processing. This will normally be in electronic form if you have made a request electronically, unless you agree otherwise.

If you request additional copies of the data provided, we will charge a fee, which will be based on the administrative cost to us of providing the additional copies.

To make a subject access request, you should complete a subject access request form a copy of which can be accessed from and should then be sent to dataprivacy@bango.com. In some cases we may need to ask for proof of identification before the request can be processed. We will inform you if we need to verify your identity and the documents we require to do this.

We will normally respond to a request within a period of one month from the date it is received. In some cases, such as where we process large amounts of your data, we may respond within three months of the date the request is received. We will write to you within one month of receiving the original request to tell you if this is the case.

If a subject access request is manifestly unfounded or excessive, we are not obliged to comply with it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which we have already responded. If you submit a request that is unfounded or excessive, we will notify you that this is the case and whether or not we will respond to it.

Other rights

You have a number of other rights in relation to your personal data. You can require us to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if your interests override our legitimate grounds for processing data
- (where we rely on our legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your interests override our legitimate grounds for processing data.

To ask us to take any of these steps, you should send the request to dataprivacy@bango.com

Data security

We take the security of your personal data seriously. We have put in place appropriate technical, physical and administrative security measures designed to provide reasonable protection of your personal data against accidental loss, unauthorised access and use, disclosure, and alteration. For example, we use firewalls, data encryption mechanisms such as SSL, and we limit physical and logical access to your personal data to those employees who have a legitimate need to access it in the proper performance of their duties and who are required to comply with our Personal Data Protection policy (HR Related Data).

Where we engage third parties to process personal data on our behalf (for example to provide you

with contractual benefits or in order to pay you), such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of your data.

Data breaches

If we discover that there has been a breach of your HR-related personal data that poses a risk to your rights and freedoms, we will report it to the Information Commissioner within 72 hours of discovery. We will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to your rights and freedoms, we will tell the affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures we have taken.

International data transfers

Your personal data may be transferred outside the European Economic Area (EEA) to The United States of America (USA). For example, if your personal data is collected, stored or processed within the cloud, server(s) or data centers of one of our global service providers such as Atlassian or Microsoft. In these circumstances the security and privacy of your personal data is safeguarded by compliance with the EU-US Privacy Shield Framework. For more information on the Privacy Shield Framework please refer to www.privacyshield.gov.

Individual responsibilities
You are responsible for helping us keep your personal data up to date. You should let us know if data provided to us changes, for example if you change your home address or bank details.

You may have access to the HR related personal data of other individuals in the course of your employment, contract, volunteer period, internship or apprenticeship. Where this is the case, we rely on you to help us meet our data protection obligations.

If you have access to HR related personal data you are required:

- to access only data that you have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have
- appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access,
- including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from
- our premises without adopting appropriate security measures (such as encryption or password
- protection) to secure the data and the device;
- not to store personal data on personal devices that are used for work purposes; and
- to report data breaches of which you become aware to Rachel Greenhalgh, Data Protection Officer
- immediately at dataprivacy@bango.com

Failing to observe these requirements may be regarded as a disciplinary offence, which will be dealt

with under our disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

The organisation will provide training to all individuals about their data protection responsibilities as part of the induction process and at periodic intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.