Phoenix
Bookkeeping & Accountancy Ltd

26 September 2018

# DATA PROTECTION POLICY

## 1. INTRODUCTION

Everyone has rights regarding how their personal information is handled. During its business activities Phoenix Bookkeeping & Accountancy Ltd (the Company) will collect, store and process personal information about employees, customers, suppliers and other third parties. The Company recognises the need to treat this information in an appropriate and lawful manner. Any breach of this policy will be taken seriously and may result in disciplinary action under the Company Disciplinary Policy and Procedure.

## 2. POLICY

This policy sets out the Company rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

If any employee considers that the policy has not been followed in respect of personal data about themselves or others, they should raise the matter with their manager.

This policy covers all employees, officers, consultants, contractors, casual workers and agency workers. It does not form part of any employee's contract of employment and the Company may amend it at any time.

## 3. PRINCIPLES

The following are terms relevant to, and used throughout, this policy:

• data: this is information which is stored electronically, on a computer, or in certain paper-based filing systems.

• data subjects: this is all living individuals about whom the Company holds personal data.

• personal data: ‘Personal data’ means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as 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 we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

• data controllers: this is the Company as it determines the purposes and the manner in which any personal data is processed.

• data users: this could include employees whose work involves using personal data. Data users have a duty to protect the information they handle at all times in accordance with this policy.

• data processors: this includes any person who processes personal data on behalf of the Company. Employees are excluded from this definition but it could include suppliers which handle personal data on the Company's behalf.

• processing: this is any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

• Special Categories of Personal Data: includes information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information - any use of special categories of personal data should be strictly controlled in accordance with this policy.
Personal data will only be collected by the Company to the extent that it is required for the specific purpose notified to the relevant data subject. Any data which is not necessary for that purpose will not be collected in the first place.

The Company shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles. The Principles are:

1. Lawful, fair and transparent: Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2. Limited for its purpose: Data can only be collected for a specific purpose.

3. Data minimisation: Any data collected must be necessary and not excessive for its purpose.

4. Accurate: The Company endeavour to ensure that personal data that is collected is accurate. Steps will be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data will be destroyed.

5. Retention: Personal data will not be kept by the Company for longer than is necessary. This means that data will be destroyed or erased from the Company systems when it is no longer required.

6. Integrity and confidentiality: The data we hold must be kept safe and secure. The Company must ensure accountability and transparency in all its use of personal data. The Company must show how they comply with each Principle. The Company is responsible for keeping a written record of how all the data processing activities it is responsible for comply with each of the Principles.

Phoenix
Bookkeeping & Accountancy Ltd

To comply with data protection laws and the accountability and transparency Principle of GDPR, the Company must demonstrate compliance. The Company is responsible for understanding its particular responsibilities to ensure they meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments
- Implement measures to ensure privacy by design and default, including:
  - Data minimisation
  - Pseudonymisation
  - Transparency
  - Allowing individuals to monitor processing
  - Creating and improving security and enhanced privacy procedures on an ongoing basis

The Company will therefore advise data subjects of the purpose for which their data is to be processed, and the identities of anyone to whom the data may be disclosed or transferred.

Where necessary, the data subject's consent to the processing will be obtained. Personal data will only be processed by the Company for the specific purposes notified to the data subject or for any other purposes specifically permitted by law. In other words, personal data will not be collected for one purpose and then used for another.

If it becomes necessary for the Company to change the purpose for which personal data is processed, the data subject will be informed of the new purpose before any processing occurs.

Individuals have rights to their data, which the Company must respect and comply with to the best of our ability. The Company must ensure individuals can exercise their rights in the following ways:

**1. Right to be informed**

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

**2. Right of access**

- Enabling individuals to access their personal data and supplementary information
- Allowing individuals to be aware of and verify the lawfulness of the processing activities

**3. Right to rectification**

- The Company must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay, and no later than one month.

**4. Right to erasure**

- The Company must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

**5. Right to restrict processing**

• The Company must comply with any request to restrict, block, or otherwise suppress the processing of personal data.

• The Company are permitted to store personal data if it has been restricted, but not process it further. The Company must retain enough data to ensure the right to restriction is respected in the future.

**6. Right to data portability**

• The Company must provide individuals with their data so that they can reuse it for their own purposes or across different services.

• The Company must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

**7. Right to object**

• The Company must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.

• The Company must respect the right of an individual to object to direct marketing, including profiling.

• The Company must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

**8. Rights in relation to automated decision making and profiling**

• The Company must respect the rights of individuals in relation to automated decision making and profiling.Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

## 4. PROCEDURE

Data about the Company's employees may be processed for legal, personnel, administrative and management purposes and to enable the Company to meet its legal obligations as an employer, for example to pay employees, monitor their performance and to confer benefits about their employment.

Examples of when sensitive personal data of employees is likely to be processed are as follows:

• information about an individual's physical or mental health or condition to monitor sick leave and take decisions as to the individual's fitness for work;

• the individual's racial or ethnic origin or religious or similar information to monitor compliance with equal opportunities legislation;

• to comply with legal requirements and obligations to third parties.

The Company will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The Company will establish procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if the third-party agrees to comply with those procedures and policies, or if they put in place adequate measures themselves.

Any employee dealing with enquiries from third parties should be careful about disclosing any personal data held by the Company. Employees should:

• check the identity of the person making the enquiry and whether they are legally entitled to receive the information they have requested;
• suggest that the third party put their request in writing so the third party's identity and entitlement to the information may be verified;
• refer to their manager for assistance in difficult situations; and
• where providing information to a third party, do so in accordance with the principles of good practice set out in this policy.

• In maintaining data security, the Company will ensure that:
• only people who are authorised to use the data can access it;
• personal data is accurate and suitable for the purpose for which it is processed; and
• only authorised persons are able to access the data if required for authorised purposes.

• All employees are responsible for ensuring that:
• where applicable, personal data is stored on the Company central computer systems instead of individual computers.
• any stranger seen in entry-controlled areas of Company's premises are reported.
• all desks and cupboards are kept locked if they hold confidential information of any kind.
• Personal data is always considered confidential.
• all paper documents are shredded and information is not transferred on to mobile devices.
• where applicable, individual computer monitors do not show confidential information to passers-by, and they log off from their computer when it is left unattended.

## 5. SUBJECT ACCESS REQUESTS

A formal request from a data subject for information that the Company holds about them must be made in writing. The Company must provide an individual with a copy of the information they requested, free of charge. This must occur without delay, and within one month of receipt. The Company will endeavour to provide data subjects access to their information in commonly used electronic formats.

The Company can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, the Company can request the individual specify the information they are requesting.

## 6. USING THIRD PARTY CONTROLLERS AND PROCESSORS

As a data controller and data processor, the Company must have written contracts in place with any third-party data controllers and/or data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

***[For controllers]*** As a data controller, the Company must only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

***[For processors]*** As a data processor, the Company must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

**Contracts**

The Company's contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. The Company's contracts with data controllers (and/or) data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

- Acting only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection
- Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations
- Nothing will be done by either the controller or processor to infringe on GDPR.

## 7. REPORTING BREACHES

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as the Company has become aware of a breach. The Company has a legal obligation to report any data breaches to Information Commissioner's Office (ICO) within 72 hours, where the breach involves special categories or data, or could lead to emotion and/or financial distress to the data subject(s).

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows the Company to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify their line manager of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

**Failure to comply**

The Company takes compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures, which may result in dismissal.

v1_PBA_PrivacyPolicy_260918