BAYtek Office Solutions Ltd
Data Protection Policy inc' Data Breach Procedure
21-5-18 v1.3

Date Of Next Review 20-5-19

1. Introduction

This Policy sets out the obligations of BAYtek Office Solutions Ltd, a company registered in United Kingdom under number 06774234, whose registered office is at 43 St Georges Road, Torquay, Devon TQ1 3QY ("the Company") regarding data protection and the rights of its employees (in this context, "employee data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "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.

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data relating to employee data subjects. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. Data Security - Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data (including, but not limited to, personal data relating to employees):

2.1 All electronic copies of personal data should be stored securely using passwords;

2.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

2.3 All personal data stored electronically should be backed up regularly with backups stored either onsite or offsite via secure hosted services. All backups will be password protected.

2.4 No personal data should be stored on any handheld device (including, but not limited to, tablets, and smartphones), whether such device belongs to the Company or otherwise. Any personal data held on Company laptops is to be password protected;

2.5 No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

3. **Data Security - Disposal**

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of under supervision of your line manager AND the IT manager in the case of electronic records.

4. **Data Security - Use of Personal Data**

The Company shall ensure that the following measures are taken with respect to the use of personal data:

4.1 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from your line manager or a Company Director;

4.2 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of your line manager or a Company Director;

4.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

4.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and

4.5 Employee personal data held by the Company will not be used for marketing purposes.

5. **Data Security - Transferring Personal Data and Communications**

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data (including, but not limited to, personal data relating to employees):

5.1 All emails containing personal data must have that data only in the form of a password protected attachment;

5.2 All emails containing personal data must be marked “confidential”;

5.3 Personal data may be transmitted over secure networks only; transmission over unsecured networks ie, public networks is not permitted in any circumstances;

5.4 Personal data may not be transmitted over a wireless network if there is a

wired alternative that is reasonably practicable;

5.5 No personal data should be contained in the body of an email, whether sent or received.

5.6 Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

5.7 Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or posted to their home address and marked as 'confidential';

5.8 All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential".

6. Data Security - IT Security and Passwords

The Company shall ensure that the following measures are taken with respect to IT and information security:

6.1 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and / or symbols;

6.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method;

6.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates;

6.4 No software may be installed on any Company-owned computer or device without the prior approval of a senior member of the IT team or a Company Director.

7. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

7.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;

7.2 Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

7.3 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

7.4 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;

7.5 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

7.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

7.7 All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;

7.8 The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

7.9 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;

7.10 All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the GDPR; and

7.11 Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

8. Transferring Personal Data to a Country Outside the EEA

8.1 The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

8.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

8.2.1 The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

8.2.2 The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

8.2.3 The transfer is made with the informed consent of the relevant employee data subject(s);

8.2.4 The transfer is necessary for the performance of a contract between the employee data subject and the Company (or for pre-contractual steps taken at the request of the employee data subject);

8.2.5 The transfer is necessary for important public interest reasons;

8.2.6 The transfer is necessary for the conduct of legal claims;

8.2.7 The transfer is necessary to protect the vital interests of the employee data subject or other individuals where the employee data subject is physically or legally unable to give their consent; or

8.2.8 The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

9. Data Breach Notification

9.1 All personal data breaches must be reported immediately to an appointed Company Director.

9.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of employee data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the appointed Company Director must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

9.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 29.2) to the rights and freedoms of employee data subjects, the Data Protection Officer must ensure that all affected employee data subjects are informed of the breach directly and without undue delay.

9.4 Data breach notifications shall include the following information:

9.4.1 The categories and approximate number of employee data subjects concerned;

9.4.2 The categories and approximate number of personal data records concerned;

9.4.3 The name and contact details of an appointed Company Director;

9.4.4 The likely consequences of the breach;

9.4.5 Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

10. **Implementation of Policy**

This Policy shall be deemed effective as of 25th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Mr Lee Hannaford

Position: Director

Date: 21-5-18

Due for Review by: 20-5-19

Signature: