Big Web Warehouse Ltd
GDPR Data Processor Policy
May 2018

1. Introduction

This Policy sets out the obligations of, Big Web Warehouse Ltd (BWW) , a company registered in the United Kingdom under number 3695066, whose registered office is at Rutland House, Minerva Business Park, PE2 6PZ ("the Company") regarding retention of personal data collected, held, and processed by the Company in accordance with 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.

The GDPR also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);

b) When the data subject withdraws their consent;

c) When the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest;

d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);

e) When the personal data has to be erased to comply with a legal obligation.

This Policy sets out the type(s) of personal data held by the Company in its capacity as a secure, archive storage provider. **The Controller decides** the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed. BWW acts on the Controllers behalf as a data **processor** to store archive material and carry out the above duties.

For further information on other aspects of data protection and compliance with GDPR, please refer to BWW's Data Protection Policy.

2. Aims and Objectives

2.1 The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Company complies fully with its obligations and the rights of data subjects under the GDPR.

2.2 In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the Company, this Policy also aims to improve the speed and efficiency of managing data.

3. Scope

a) This Policy applies to all personal data held by BWW's in it's capacity as a third party data processor.The Controller holds databases which are only disclosed to BWW if chosen to do so. The data is requested by the Controller by a computerised bar code of a specific box/file and cross reference to the nature of the content is not required by the Processor to operate the service (pseudonymisation).

3.2 Personal data, as held by BWW is stored in the following ways and in the following locations:

b) The Company's servers, located at Harrier Park (and secondary secure location).

c) Computers permanently located in the Company's premises at Harrier Park and Tresham Road.

d) Physical records stored at BWW premises.

4. Data Subject Rights and Data Integrity

All personal data held by the Company is held in accordance with the requirements of the GDPR and data subjects' rights there under, as set out in the Company's Data Protection Policy.

5. Technical and Organisational Data Security Measures

5.1 The following technical measures are in place within the Company to protect the security of personal data. Please refer to BWW's Data Protection Policy.

a) Personal data may only be transmitted over secure networks;

b) Where personal data is to be transferred in hardcopy form, it should be collected and delivered to the Controllers premises in BWW tracked, unmarked vehicles or as directed by the Controller.

c) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested by the Controller.

d) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;

e) 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 authorisation;

f) Personal data must be handled with care at all times and should not be left unattended or on view;

g) Computers used to view personal data must always be locked before being left unattended;

h) No personal data should be stored on any mobile device, whether such device belongs to the Company or otherwise.

i) All personal data stored electronically should be backed up daily with backups stored on and off site.

j) All electronic copies of personal data should be stored securely using passwords.

k) All passwords used to protect personal data should be changed regularly and should be secure;

l) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method.

m) All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible.

n) No software may be installed on any Company-owned computer or device without approval.

5.2 The following organisational measures are in place within the Company to protect the security of personal data.

a) All employees and 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 the Company's Data Protection Policy;

b) Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company;

c) All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

d) All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised;

e) All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times;

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

g) The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

h) All employees and other parties working on behalf of the Company handling

personal data will be bound by contract to comply with the GDPR and the Company's Data Protection Policy.

6. **Data Disposal**

The Controller governs the expiry of the data retention periods set out below in Part 7 of this Policy, or when personal data shall be deleted, destroyed, or otherwise disposed of as follows:

6.1 Personal data stored electronically (including any and all backups thereof) shall be deleted securely ;

6.2 Personal data stored in hardcopy form shall be shredded to BS EN15713 and recycled.

7. **Data Retention**

7.1 As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed and is governed by the Controller.

7.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods **(**and its retention periodically reviewed), as set out below.

7.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

a) The objectives and requirements of the Controller;

b) The type of personal data in question;

c) The purpose(s) for which the data in question is collected, held, and processed;

d) BWW's legal basis for collecting, holding, and processing that data;

7.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

7.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made by the Controller to do so (whether in response to a request by a data subject or otherwise).

7.6 In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

8. **Roles and Responsibilities**

8.1 The Company's Data Protection Officer is Mrs.J.Lester, Director,Unit A Harrier Park,Orton Southgate, Peterborough,PE2 6YQ.

8.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.

8.3 The Data Protection Officer shall be directly responsible for ensuring compliance.

8.4 Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.

9. **Implementation of Policy**

This Policy shall be deemed effective as of 1st 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: J.Lester

Position: Director

Date: 01 May 2018

Due for Review by: 01 May 2019

Signature: