People Based Solutions
Data Retention Policy
1st May 2018

1. Introduction

This Policy sets out the data retention obligations of People Based Solutions Ltd regarding the personal data of its customers, customers' employees, prospective employees and business contacts under all applicable Privacy Laws.

2. Definitions and Interpretation

"The Company" means People Based Solutions Ltd., a company registered in England and Wales under number 08065344, whose registered office is at Dallam Court, Dallam Lane, Warrington, Cheshire, WA2 7LT

"Privacy Laws" means all applicable privacy and data protection laws including the EU Regulations, General Data Protection Regulation ("GDPR") and the Privacy and Electronic Communications (EC Directive) Regulation 2003 (as amended), together with the Data Protection Act 2018 and all subordinate legislation, directions of any competent privacy regulator, common law and other relevant court decisions and all relevant privacy and/or data protection codes of practice in each case as may be amended or replaced from time to time.

"Personal data" means any information relating to an identifiable natural person who can be directly or indirectly identified from that information ('the data subject"). This definition shall, where applicable, incorporate the definitions provided in the "GDPR"; and in this case, it applies to personal data disclosed to the Company for the purposes of managing the provision of its services.

"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.

"Data retention" means when the Company holds personal data according to the applicable Privacy Laws, ensuring in particular, that personal data are adequate, relevant, accurate and up to date and are held for no longer than is necessary for the purposes for which the personal data is processed. (See Section 7 of this policy)

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 to protect that data. (See section 5 of this policy).

"The right to erasure" (or "the right to be forgotten") means data subjects have the right to have their personal data erased, and to prevent the processing of that personal data. (See section 5 of this policy)

3. Aims and Objectives

This primary aims of this policy are to:

3.1 Establish the periods of time for which personal data is to be retained and the criteria for establishing and reviewing such periods.

3.2 Ensure that out of date, irrelevant, inaccurate and excessive amounts of data are not retained by the Company.

3.3 Improve the speed and efficiency of managing data and index systems.

3.4 Safeguard data subjects' rights under the applicable Privacy Laws.

4. Scope

4.1 This Policy applies to all personal data held by the Company, joint data controllers or data controllers – in common; and by any third-party processing personal data on the Company's behalf, including but not limited to, data processors, sub data processors and contractors.

4.2 Personal data may recorded in any of the following:

a) documents (including written and typed documents and annotated copies)

b) Computer files (including word processor files, databases, spreadsheets and presentations)

c) Records contained in computer systems e.g. HR, training and finance

d) Paper based files

e) Email and Instant messages

f) Calendar records

g) Reports

h) Voice recordings (including call recording)

i) Internal and external web-chat

j) Intranet and Internet Web pages

k) Screen sharing

4.3 Personal data, processed by the Company are stored in the following ways in the following locations:

a) Computer hardware and mobile devices, including, but not limited to, laptops, tablets and smart phones provided by the Company to its employees and any third parties contracted to the Company;

b)

Third-party servers, operated by 123 Reg a limited company registered in England under company number 05306504, 5th Floor, The Shipping Building Old Vinyl Factory, 252-254 Blyth Road, Hayes, Middlesex, UB3 1HA and hosted

within the European Union;

c) Computer hardware including, but not limited to servers, PC's and laptops, operated by Techniframe Ltd, a limited company registered in England under company number 08936951, whose registered address is Ashland House, Dobson Park Way, Ince in Makerfield, Wigan, WN2 2DX

d) Electronic contracts stored online on the PBS CRM system which is hosted by 123 Reg and hosted within the European Union

e) Client and supplier financial information operated by Quickbooks Online a limited company registered in England under company number, 2679414, whose registered address is 1 Cathedral Piazza, London, SW1E 5B and hosted within the European Union.

f) Employee payroll information help and processed by AIMS accountancy services a limited company registered in England under company number, 02740695, whose registered address is 3 Park Road, London, NW1 6AS and hosted within the European Union.

5. Data Subject Rights and Data Integrity

All personal data held by the Company is held in accordance with the requirements of the applicable Privacy Laws and data subjects' rights thereunder, as set out in the Company's Data Protection Policy.

5.1 Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is used as set out in Parts 12 and 13 of the Company's Data Protection Policy, and how long the Company will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

5.2 Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to restrict the Company's use of their personal data and the right to data portability.

5.3 Data subjects also have the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy) in the following circumstances:

a) Where the personal data are no longer required for the purpose for which it was originally collected or processed;

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 are processed unlawfully (i.e. in breach of the GDPR);

e) When the personal data have to be erased to comply with a legal obligation; or

Where the personal data are processed for the provision of information society services to a child.

6. Technical and Organisational Data Security Measures

6.1 The following technical measures are in place within the Company to protect the security of personal data. Please refer to Parts 22 to 26 of the Company's

Data Protection Policy for further details:

a) All emails containing personal data must be encrypted;

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

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

d) Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;

e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;

f) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;

g) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using Royal Mail Registered Post;

h) All personal data transferred physically should be transferred in a suitable container marked “confidential”;

i) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from The Managing Director.

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

k) 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 written authorisation from the Data Protection Officer;

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

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

n) Personal data in digital format should be accessed via double-authentication.

o) No personal data should be stored on any mobile device, whether such device belongs to the Company or otherwise without the formal written approval of the Data Protection Officer and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;

p) No personal data should be transferred to any device personally belonging to an employee, agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the Company’s Data Protection Policy and the Privacy Policy without the formal written approval of the Data Protection Officer and on condition the data is permanently deleted from such a device once the employee, agent, contractor or other third party has left the premises of the Company

q) All personal data stored electronically should be backed up twice weekly with backups stored on Techniframe servers All backups should be encrypted;

r) All electronic copies of personal data should be stored securely using passwords and encryption;

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

t) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

u) All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after their release;

v) No software may be installed on any Company-owned computer or device without approval; and

w) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Managing Director to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

6.2 The following organisational measures are in place within the Company to protect the security of personal data. Please refer to Paragraph 27 of the Company's Data Protection Policy for further details:

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;

i) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the GDPR and the Company's Data Protection Policy;

j) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under the GDPR and/or the Company's Data Protection 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.

7. **Data Disposal**

Upon the expiry of the data retention periods set out below in Part 8 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

7.1 Personal data stored electronically (including any and all backups thereof) shall be deleted securely. Data held in database table will be deleted using the DBMS delete process, all associated linked data would be deleted in the same way. Data held in files would be deleted using the system operating system delete function including folders relating to the individual.

7.2 Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely. Personal data stored electronically (including any and all backups thereof) shall be deleted securely. Data held in database table will be deleted using the DBMS delete process, all associated linked data would be deleted in the same way. Data held in files would be deleted using the system operating system delete function including folders relating to the individual.

7.3 Personal data stored in hardcopy form shall be shredded BSEN 15713 shred no 3, which is a shred width of no more than 16mm and recycled;

7.4 Special category personal data stored in hardcopy form shall be shredded **[**to at least BSEN 15713 shred no 4 which is a shred width of no more than 12mm and recycled**.**

8. Data Retention

8.1 As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary for the purpose(s) for which that data was originally collected.

8.2 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.

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

a) The objectives and requirements of the Company;

b) The type of personal data in question;

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

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

e) The category or categories of data subject to whom the data relates;

8.4 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.

8.5 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 within the Company to do so (whether in response to a request by a data subject or otherwise).

Type of Data	Purpose of Data	Review Period	Retention Period or Criteria	Comments
Customer employee Name, employer, job title, e-mail, work telephone number	To create user profiles to allow customers to access the Company's on-line services, including the help desk, the client document library, and the HR software suite. To send e-mail messages and links to blogs and news letters to keep them up to date with best practice and any new services being developed or offered by the Company	Annually	3 months after the employing organisation is no longer a customer of the Company, 3 months after the data subject is no longer employed by the Company's customer 3 months after the data subject is moved to a post within the customer company that does not liaise with the Company	We keep the data of end user no longer than is necessary. If for any reason a user is no longer active, we keep their data for no longer than 12 weeks from that date we are aware that they are no longer active.
Prospective customer employees' Name, employer, job title, work e-mail,	To send e-mail marketing messages and links to blogs and news letters to promote the Company's services and new offers being developed by the Company	Annually	12 months from the expressed agreement to remain on the mailing list.	Prospective employees' customers must opt in and can have their records deleted at any time either by unsubscribing or requesting the record is deleted.

Type of Data	Purpose of Data	Review Period	Retention Period or Criteria	Comments
Customer Employee name and job title	To draft correspondence to the Company's customers employees.	Quarterly	4 weeks from the date the information is received	We do not keep personal information on customers' employees for any other purpose than to produce correspondence on our customers behalf. Our aim is to delete it as soon as possible. 4 weeks is the longest we will keep it.
Applicants for employment or prospective employees with the Company's customer: name and address	To draft employment contracts, draft offer letters and seek reference requests for prospective employees.	Quarterly	4 weeks from the date the information is received	We do not keep personal information on applicants for employment or prospective employees with our customers for any other purpose than to produce correspondence on our customers behalf, and occasionally seek references. We do not keep lists of those interested in seeking employment with our clients. We will delete the data as soon as possible. 4 weeks is the longest we will keep it.
Company Employee's	To maintain our contractual and legal obligations with the employee. To fulfil our legal obligations under UK Employment Law and Th Health and Safety at Work Act. To comply with our legal and regulatory obligations to 3rd parties and government bodies such as HMRC. To meet the legitimate aims of the Company to maximise	Annually	6 years from the date the employee leaves the Company	Employee data will be held in line with the employee data retention schedule attached at Appendix 1

	efficiency and manage performance			

9. **Roles and Responsibilities**

9.1 The Company's Data Protection Officer is Sean McCann Managing Director, smccann@peoplebasedsolutions.com.

9.2 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.

9.3 The Data Protection Officer shall be directly responsible for ensuring compliance with the above data retention periods throughout the Company**]**.

9.4 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.

10. **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.