Data Retention Policy
Aaron Wallis Sales Recruitment

Policy Name:	Data Retention Policy
Date Created	3/5/2018
Prepared by:	George Humphries, Data Protection Co-Ordinator
Approved by:	Robert Scott, Managing Director
Policy owner:	Robert Scott, Managing Director

AARON WALLIS
SALES RECRUITMENT

1. Introduction

This Policy sets out the obligations of Aaron Wallis Sales Recruitment, ("the Company") a company registered in England, under number No. 6356563, whose registered office is at: Stratford Business Village, 23 Walker Avenue, Wolverton Mill, Milton Keynes, MK12 5TW 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; or

f) Where the personal data is processed for the provision of information society services to a child.

This Policy sets out the type(s) of personal data held by the Company purposes 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 of.

For further information on other aspects of data protection and compliance with the GDPR, please refer to the Company'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**

3.1 This Policy applies to all personal data held by Aaron Wallis Sales Recruitment and by third-party data processors processing personal data on the Company's behalf.

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

a) Third-party servers, operated by and located at address: Host-IT Internet Solutions, Unit 1, Northampton Science Park, Moulton Park Industrial Estate, Northampton, NN3 6LG

b) Computers permanently located in the Company's premises at: Stratford Business Village, 23 Walker Avenue, Wolverton Mill, Milton Keynes, MK12 5TW

c) Laptop computers, and other mobile devices**,** provided by the Company to its employees;

d) Third-party Employment Checking Agency – KnowYourCandidate

e) CRM Provider – Bullhorn

f) Applicant Tracking System – Broadbean

g) Back Office Systems and Accounts Consultancy - SimplicityinBusiness

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 thereunder, as set out in the Company's Data Protection Policy.

4.1 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).

4.2 Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Company's use of their personal data, the right to data portability, and further rights relating to automated decision-making and profiling , as set out in Parts 14 to 20 of 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 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 SSLUpload (https://sslupload.co.uk/);

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 Robert Scott, Data Protection Officer;

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 authorisation;

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) 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 Managing Director 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;

o) All personal data stored electronically should be transferred onto Bullhorn, the CRM system and encrypted as soon as feasibly possible;

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

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

r) 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;

s) All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;

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

u) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of Robert Scott, Data Protection Officer, 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.

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

6. **Data Disposal**

Upon the expiry of the data retention periods set out below in Part 7 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:

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

6.2 Personal data stored in hardcopy form shall be shredded and recycled;

6.3 Special category personal data stored in hardcopy form shall be shredded the highest CESG/DIPCOG HDD erasure standards. Current Supplier is: Box-It South Midlands;

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.

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 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;

f) Additional considerations as detailed in the Company GDPR Data Protection Policy;

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

7.6 In limited circumstances, such as placed permanent candidates. it may also be necessary to retain personal data for longer periods where such retention is required by HMRC, unless request to be forgotten is received.. 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. This is a legal requirement also under the Conduct of Employment Agencies and Employment Business Regulations;

7.7 Candidate applications to adverts via Aplitrak (Broadbean), and Candidates sourced from third party CV databases and stored 'shortlisted' against a job in Aplitrak can be retained for up to default 6 months from the point of application

or import.

7.8 Candidates transferred to Talent Search (BroadBean) will be retained for 2 years from the point they enter the system;

7.9 Within Talent Search, this period will be reset if the same candidate is re-entered into the system via a new application, if their details are subsequently downloaded from an external CV database channel, or if their details re-enter the system through other imports;

7.10 Candidates transferred to Bullhorn (Recruitment CRM) will be retained for 2 years from the point they enter the system;

7.11 Candidate applications via aaronwallis.co.uk and transferred onto Bullhorn (Recruitment CRM) will be retained for 2 years from the point they enter the system;

7.12 In all cases, when candidate records expire, the candidate Personal Information will be automatically deleted from the Broadbean system (Aplitrak and Talentsearch). They are removed or anonymised in such a way that while no Personal Data will remain, we will still be able to report accurately the fact that a candidate application event occurred against the relevant advert from a specific channel. The same process takes place upon receiving a withdraw of consent application.

7.13 In all cases, when candidate records expire, the candidate Personal Information will be automatically anonymised from the Bullhorn Recruitment CRM system. When a candidate is anonymised, the request is captured and stored in the system. Erasure will replace the candidate's identifiable data with either asterisks (****) or a random string of characters (e.g. ATgl1523900220). Date fields will be replaced with the date the record was erased. The same process takes place upon receiving a withdraw of consent application.

Section number	Explanation
Sensitive personal data	The Data Protection Act 1998 (DPA) uses the term 'sensitive personal data' which includes information on an individual's physical and mental health, sexual orientation, race or ethnic origin, religious beliefs, trade union membership and criminal records. Our standard process requires us to store the following data: **Personal data** • Name (first and last names are mandatory, middle names are optional) • Date of birth • Contact details, including telephone number, email address and postal address • Gender • Experience, training and qualifications • CV • Right to work check / Immigration permission to work in the UK • National insurance number (or date of birth and gender if no National Insurance no.) • IP Address • Driving Licence and points on driving license (if applicable to the role) **Sensitive personal data** • Disability/health condition relevant to the role • Criminal conviction
Data processing under the Data Protection Laws	ICO Registration Number: Z1059320

Legal bases for processing	The Company processes personal data in relation to its own staff, work-seekers and individual client contacts and is a data controller for the purposes of the Data Protection Laws. The Company has registered with the ICO. The Company may hold personal data on individuals for the following purposes: • Staff administration; • Advertising, marketing and public relations • Accounts and records; • Administration and processing of work-seekers' personal data for the purposes of providing work-finding services, including processing using software solution providers and back office support; • Administration and processing of clients' personal data for the purposes of supplying/introducing work-seekers; 1. The data protection principles The Data Protection Laws require the Company acting as either data controller or data processor to process data in accordance with the principles of data protection. These require that personal data is: 1. Processed lawfully, fairly and in a transparent manner; 2. Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes; 3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; 4. Accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; 5. Kept for no longer than is necessary for the purposes for which the personal data are processed; 6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and that 7. The data controller shall be responsible for, and be able to demonstrate, compliance with the principles.

	2. Legal bases for processing The Company will only process personal data where it has a legal basis for doing so. Where the Company does not have a legal reason for processing personal data any processing will be a breach of the Data Protection Laws. The Company will review the personal data it holds on a regular basis to ensure it is being lawfully processed and it is accurate, relevant and up to date and those people listed in the Appendix shall be responsible for doing this. Before transferring personal data to any third party (such as past, current or prospective employers, suppliers, customers and clients, intermediaries such as umbrella companies, persons making an enquiry or complaint and any other third party (such as software solutions providers and back office support)), the Company will establish that it has a legal reason for making the transfer.
Privacy notices	Website Privacy Policy - https://www.aaronwallis.co.uk/privacy-policy.aspx Candidate Privacy Notice - https://www.aaronwallis.co.uk/candidate-privacy-notice
Subject access requests	Individuals will have the right to obtain information that an organisation holds on them under what is known as a subject access request. The form can be completed here: https://www.aaronwallis.co.uk/sar
Rectification	See Data Protection Procedure and process to withdraw consent is available at: https://www.aaronwallis.co.uk/Withdrawal-of-Consent.aspx
Erasure	See Data Protection Procedure and process to withdraw consent is available at: https://www.aaronwallis.co.uk/Withdrawal-of-Consent.aspx
Restriction of processing	See Data Protection Procedure
Data portability	See Data Protection Procedure
Object to processing	Individuals will have the right to ask *data controllers* to object to the processing of their personal data and withdraw their consent. See Data Protection Procedure and process to withdraw consent is available at: https://www.aaronwallis.co.uk/Withdrawal-of-Consent.aspx

Client Contact Information	Sourced by • Marketing initiatives including online advertising and remarketing; • 3rd Party Sites; • Information in the public domain; • Social Media Sites; • In person meetings; • Telephone conversations; • Email correspondence; • Video meetings; • Recruitment workflows & outcomes including reference requests; • Hiring Preferences; • Vacancy descriptions /requirements; • Canvass calls; • Profile Images; See Data Protection Procedure and process to withdraw consent is available at: https://www.aaronwallis.co.uk/Withdrawal-of-Consent.aspx Individuals will have the right to obtain information that an organisation holds on them under what is known as a subject access request. The form can be completed here: https://www.aaronwallis.co.uk/sar
Terms of Business with Clients	6 Years (In order to deal with any civil action in the form of a contractual claim.)

8. **Roles and Responsibilities**

8.1 The Company's Data Protection Officer is Robert Scott, Data Protection Officer, gdpr@aaronwallis.co.uk, 01908 061400, Aaron Wallis, Stratford Business Village, 23 Walker Avenue, Wolverton Mill, Milton Keynes, MK12 5TW

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 with the above data retention periods.

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 24th 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: Robert Scott

Position: Managing Director and Data Protection Officer

Date: 24th May 2018

Due for Review by: 3rd November 2018

Signature:

Revision History

Date of Change	Editor	Summary of Change	Date of next revision
May 3rd 2018	George Humphries (Data Protection Co-Ordinator)	Updated and converted to new format.	November 3rd 2018