Data Retention Policy

1. Purpose, Scope, and Users

This policy sets the required retention periods for specified categories of personal data and sets out the minimum standards to be applied when destroying certain information within the BABA.

This Policy applies to all employees, contractors and consultants that may collect, process, or have access to data (including personal data and/or sensitive personal data). It is the responsibility of all the above to familiarise themselves with this Policy and ensure adequate compliance with it.

This policy applies to all information used at the BABA. Examples of documents include:

- Emails
- Hard copy documents
- Soft copy documents
- Video and photographs

2. Retention Rules

Retention General Principle

In the event, for any category of documents not specifically defined elsewhere in this Policy (and within the Data Retention Schedule) and unless otherwise mandated differently by applicable law, the required retention period for such document will be deemed to be 3 years from the date of creation of the document.

Retention General Schedule

BABA defines the time period for which the documents and electronic records should to be retained through the Data Retention Schedule.

As an exemption, retention periods within Data Retention Schedule can be prolonged in cases such as:

- If there is a chance records of personal data are needed by the Company to prove compliance with any legal requirements; or

- When exercising legal rights in cases of lawsuits or similar court proceeding recognized under local law.

Destruction of Data

The BABA should on a regular basis, review all data, whether held electronically on their device or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant. See Appendix for the retention schedule. Overall responsibility for the destruction of data falls to the Head of Operations.

Once the decision is made to dispose according to the Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal varies and is dependent upon the nature of the document. For example, any documents that contain sensitive or confidential information (and particularly sensitive personal data) must be disposed of as confidential waste and be subject to secure electronic deletion; some expired or superseded contracts may only warrant in-house shredding. The Document Disposal Schedule section below defines the mode of disposal.

The Head of Operations shall fully document and approve the destruction process. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed.

Breach, Enforcement and Compliance

The person appointed with responsibility for Data Protection, has the responsibility to ensure that all BABA employees comply with this Policy. It is also the responsibility of the Head of Operations to assist with enquiries from any local data protection or governmental authority.

Any suspicion of a breach of this Policy must be reported immediately to the Head of Operations. All instances of suspected breaches of the Policy shall be investigated and action taken as appropriate.
Failure to comply with this Policy may result in adverse consequences, including, but not limited to, litigation, financial loss and damage to the Company`s reputation, personal injury, harm or loss. Non-compliance with this Policy by permanent, temporary or contract employees, or any third parties, who have been granted access to BABA premises or information, may therefore result in disciplinary proceedings or termination of their employment or contract. Such non-compliance may also lead to legal action against the parties involved in such activities.

3. Document Disposal

Destruction Method

Level I documents are those that contain information that is of the highest security and confidentiality and those that include any personal data. These documents shall be disposed of as confidential waste (cross-cut shredded and incinerated) and shall be subject to secure electronic deletion. Disposal of the documents should include proof of destruction.

Level II documents are proprietary documents that contain confidential information such as parties` names, signatures and addresses, or which could be used by third parties to commit fraud, but which do not contain any personal data. The documents should be cross-cut shredded and then placed into locked rubbish bins for

collection by an approved disposal firm, and electronic documents will be subject to secure electronic deletion.

Level III documents are those that do not contain any confidential information or personal data and are published Company documents. These should be strip-shredded or disposed of through a recycling company and include, among other things, advertisements, catalogues, flyers, and newsletters. These may be disposed of without an audit trail.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Data Retention Schedule	Head of Operations sharepoint	Head of Operations	Only authorised persons may access this document	Permanently

5. Validity and document management

This document is valid as of May 2018

The owner of this document is the Head of Operations who must check and, if necessary, update the document at least once a year.

6. Appendices

Appendix – Data Retention Schedule

Financial Records

Personal data record category	Mandated retention period	Record owner
Payroll records	Seven years after audit	Finance
Supplier contracts	Seven years after contract is terminated	Finance
BABA Policies and Procedures	Permanent	Finance
Permanent Audits	Permanent	Finance

Financial statements	Permanent	Finance
General Ledger	Permanent	Finance
Investment records (deposits, earnings, withdrawals)	7 years	Finance
Invoices	7 years	Finance
Cancelled checks	7 years	Finance
Bank deposit slips	7 years	Finance
Business expenses documents	7 years	Finance
Property/asset inventories	7 years	Finance
Credit card receipts	3 years	Finance
Petty cash receipts/documents	3 years	Finance

Business Records

Personal data record category	Mandated retention period	Record owner
Board policies	Permanent	Finance
Board meeting minutes	Permanent	Finance
Tax or employee identification number designation	Permanent	Finance
Office and team meeting minutes		Finance
Annual corporate filings	Permanent	Finance

HR: Employee Records

Personal data record category	Mandated retention period	Record owner
Disciplinary, grievance proceedings records, oral/verbal, written, final warnings, appeals	As per legal requirement	HR
Applications for jobs, interview notes – Recruitment/promotion panel Internal Where the candidate is unsuccessful Where the candidate is successful	Deleted immediately Duration of employment	HR
Payroll input forms, wages/salary records, overtime/bonus payments Payroll sheets, copies	7 years	HR
Bank details – current	Duration of employment	HR
Payrolls/wages	Duration of employment	HR
Job history including staff personal records: contract(s), Ts & Cs; previous service dates; pay and pension history, pension estimates, resignation/termination letters	As per legal requirement	HR
Employee address details	Duration of employment	HR
Expense claims	As per legal requirement	HR
Annual leave records	Duration of employment	HR
Accident books Accident reports and correspondence	As per legal requirement	HR
Certificates and self-certificates unrelated to workplace injury; statutory sick pay forms	As per legal requirement	HR

Pregnancy/childbirth certification	As per legal requirement	HR
Parental leave	Duration of employment	HR
Maternity pay records and calculations	As per legal requirement	HR
Redundancy details, payment calculations, refunds, notifications	As per legal requirement	HR
Training and development records	Duration of employment	HR

Contracts

Personal data record category	Mandated retention period	Record owner
Signed	Permanent	Finance
Contract amendments	Permanent	Finance
Successful tender documents	Permanent	Finance
Unsuccessful tenders` documents	Permanent	Finance

Athlete Data

Personal data record category	Mandated retention period	Record owner
Inclusive of Passport details, email addresses, first and second names, address	Retained whilst athlete is on WCPP and/or Professional Programme. Once athlete is released from programme all records to be deleted, data will be removed from the back-ups within 9 months	Athlete

Non – Athlete Data

Personal data record category	Mandated retention period	Record owner

Name, email address	Kept until person unsubscribes / requests to be removed from system	Marketing

IT

Personal data record category	Mandated retention period	Record owner
Recycle Bins	Cleared monthly	Individual employee
Downloads	Cleared monthly	Individual employee
Inbox	All emails containing PII attachments deleted after 3 years.	Individual employee
Deleted Emails	Cleared monthly	Individual employee
Personal Network Drive	Reviewed quarterly, any documents containing PII deleted after 3 years	Individual employee
Local Drives & files	Moved to network drive monthly, then deleted from local drive	Individual employee
Google Drives, drop box	Reviewed quarterly, any documents containing PII deleted after 3 years	Individual employee