Document and Data Retention Policy

Policy Reference:

BP027

Approved by:

Audit and Risk Committee

Date approved:

23 April 2018

1. Scope and Objectives

This policy sets out how data and documents, which are controlled or processed by bpha and its subsidiary companies (bpha, the group, we or us), will be managed through retention, storage and disposal.

This applies to all documents and data that bpha possess, from creation to destruction, inclusive of whether the data or documents are printed, written on paper or stored electronically/digitally, regardless of whether the data or documents are personal, confidential, or any other type of data.

bpha's specific policy objectives are:

- To ensure compliance with the General Data Protection Regulations 2018 and the Data Protection Act 1998
- To protect Data Subject Rights
- To prevent the storage of documents or data longer then is lawfully required
- To ensure that retention schedules are consistent with what is stated when the data is gathered
- To prevent unlawful or premature destruction of personal, corporate and other types of data
- To promote good Records Management practices within bpha.

2. Policy Statement

To provide the comprehensive range of services that bpha delivers, the retention, storage and disposal of data will be undertaken at appropriate times, with adequate methods to meet our legislative, regulative and any other significant obligations.

bpha needs to process data and use documentation to be able to provide its services. This requires information to be stored in systems that enable it to honour contracts and service agreements. bpha will only hold data and documentation for as long as required and will deploy an effective review mechanism to ensure that this works in practice.

bpha will ensure compliance with all necessary regulatory and legislative requirements regarding data and document retention, storage and disposal.

3. Roles and Responsibilities

The **Board** are responsible for:

- taking ownership of responsibility for data and document retention within bpha, and leading by example.
- Regularly reviewing bpha's data and document retention policy and data retention schedule.

The **Audit and Risk Committee** are responsible for:

- monitoring the adherence to policy through regular reporting to the Committee.

The **Director of IT** is responsible for:

- the security and maintenance of the IT Infrastructure and Cyber Security Landscape.

Data Owners are responsible for:

- creating and maintaining the data retention schedule for their area
- ensuring data and documents are managed in line with their relevant data retention schedule
- ensuring data and documents are disposed of, and that disposal is appropriate for the type of data
- appointing a data steward.
- ensuring that logs are maintained for Special Categories of Personal Data within their area.

Data Owners and their remits are detailed in the table below:

Data Owner Role	Remit
Head of Communications	Corporate related communication, websites, and images/footage.
Head of Development	Development documentation
Head of Finance	Financial records and returns, including tax, invoices, journals, and payment related information.
Head of Governance and Legal	Documentation related to Procurement, Governance, Contracts, Board, Policy, and Legal correspondence and matters.
Head of Home Ownership	Leases (current and former), Deeds of Ownership, and Help to Buy Documents.
Head of Housing Operations	Tenancy and Applicant files (current and former), care plans, ASB cases, rent statements, tenant and applicant correspondence.
Head of Human Resources	Any item that is Employee (current, former and prospective) related
Head of Property Services	Property maintenance records, building control information and reports and professional opinions relating to property.
Head of Retirement Living	Nursing home and residential care homes related documentation.
Head of Treasury	Business plans & supporting documentation, valuation, insurance (coverage and claims), funding (bonds, grant, loads), regulator returns and Ownership related documentation.

Health, Safety, Environment and Facilities Manager	Health and Safety records, vehicle MOT and registration.
Quality and Assurance Manager	Standards (e.g. ISO), audit, risk, project management related documentation

Data Stewards are responsible for:

- day-to-day responsibility for ensuring compliance to the Data and Document Retention Policy and Schedule.

The **Data Protection Officer** (DPO) is responsible for:

- monitoring and reporting to senior management on data and document retention policy compliance
- regular auditing of different business units to ensure compliance

All **employees** are responsible for:

- working in accordance with data and document retention policies, procedures and schedule.

4. Policy Details

4.1. TYPES OF DOCUMENT

bpha processes and stores a wide range of data and documentation. This includes, but is not limited to:

- Handwritten notes
- E-mails
- Letters and correspondence
- Invoices and financial statements
- Proof of identification and medical information
- Memory in mobile devices, computer hardware and backup
- Computer programmes
- Call Recordings/voicemail
- Surveillance footage
- Online postings on social media platforms or websites

4.2. RETENTION

This policy ensures that the periods identified in the Data and Document Retention Schedule are enforced and that documents or data are not prematurely destroyed.

Documents and data will be retained in secure locations and in the appropriate format to meet its purpose. Electronic copies will be minimised to a single copy where possible, with paper documents retained for legal or contractual purposes only.

4.3. DISPOSAL

Data and Documentation, whether paper or electronic, will be disposed of in line with the Schedules detailed in bpha's Data and Document Retention Schedule. bpha will take every opportunity to automate the review and disposal process.

A record of document and data disposal will be retained to confirm the implementation of these guidelines.

Paper copies will be confidentially and securely destroyed with a certificate of destruction where practical. Digital, electronic or hardware containing data will be disposed of in co-ordination with the IT department aligned to National Archive guidelines.

4.4. STORAGE

bpha will ensure that data is stored in a way that meets the principle of "Secure by Design". Robust security protocols and safeguards will be applied regardless of storage type or location (e.g. paper, device, system).

bpha will seek to store as few copies of the same documentation and data as possible. The location of data and documentation storage will comply with the GDPR.

4.5. CONSENT

Where consent is required for the storage and processing of data, the withdrawal of consent will mean that data will be erased or returned. In the event that processing is solely reliant on consent, this Data Subject Right overrides this policy and bpha's Data and Document Retention Schedule.

4.6. 3RD PARTY DATA SHARING

bpha will ensure that where data is shared with 3rd parties , they will follow bpha's Data and Document Retention Policy. This will identify where data needs to be deleted or returned by the Data Processor. This will be enforced through legally binding contracts.

Where bpha are the Data Processor, we will comply with the Data Controllers Data Retention, Storage and Disposal requirements where they are aligned with our contractual, regulatory and legislative obligations. This will be defined in the pre-contract signing stage.

bpha will not share personally identifiable or personal information without a legally binding contract or regulatory/legal imperative.

4.7. IMAGES AND RECORDINGS

bpha sometimes need to record calls and gather photographic images/recordings to fulfil our obligations.

4.7.1. Call Recording

All calls that are handled through the Automatic Call Distribution (ACD) are recorded. bpha ensures that a clear welcome message details the purpose and usage of call recording. Calls will be automatically deleted after a period of 6 months. The retention period for specific calls may be extended based upon where callers have been abusive or problematic, or where complaints or legal claims have been received or are expected. The retention of all such calls will be reviewed monthly, and calls will be deleted where they are no longer required.

Monitoring of call recordings will be undertaken by authorised employees on a need to know basis to ensure policy adherence, meeting bpha's obligations and for staff development.

Call recording files will not be removed from the Call Recording system, unless there is an overriding imperative to do so.

4.7.2. Closed circuit television (CCTV)

bpha utilises CCTV and photographic images for a variety of legitimate reasons including, but not limited to, prevention or detection of crime or disorder to identifying service needs (e.g. fly-tipping).

Before CCTV systems are installed, a CCTV Impact Assessment will be carried out. This will ensure the system is compliant with the GDPR. A master list of all CCTV systems is held by the Data Protection Officer.

CCTV recordings will be automatically deleted after a maximum of 6 months, unless there is an investigation, legal and/or regulatory requirement or request for the footage from a particular system. CCTV recordings will only be shared with 3rd parties in line with section 5.

4.7.3. Photographic images (excluding CCTV)

bpha employees are provided with devices, where required, that contain the ability to capture and store photographic images and video recordings. All bpha staff receive annual Data Protection training and will only take photographic images or recordings with people identifiable where necessary.

Employees must ensure that photographic images and recordings are held only as long as required by bpha's Data and Document Retention Schedule. If the images or recordings are used in a form of corporate publication, a photographic consent form will be required before usage.

4.8. SPECIAL CATEGORIES OF PERSONAL DATA

The GDPR identifies "Special Categories of Personal Data". These merit special protection and a significant restriction of processing.

bpha will ensure that these are only gathered in line with our legal responsibilities or within the acceptable use of Special Categories of Personal Data identified within the GDPR.

Where bpha collects this information for a specific purpose this will be identified on logs so that all Special Category of Personal Data is tracked, monitored and deleted after it's requirement. bpha will ensure that there are an appropriate number of logs to prevent unnecessary access to such data. This will be overseen by the Data Protection Officer.

4.9. EXCEPTIONS

For personal data, there are three exceptions to this policy.

- Consent has already been mentioned as an exception to this policy under section 4.
- Where data or documentation needs to be retained for establishment or defence of legal claims.
- User discretion over temporary data or documents. This includes duplicates of originals also preliminary drafts of letters, spreadsheets, or informal notes that do not represent significant steps or decisions towards making official records.

5. Regulatory and legal Considerations

General Data Protection Regulations 2018
Data Protection Act 1998
CCTV Code of Practice produced by ICO
Human Rights Act 1998
Regulation of Investigatory Powers Act 2000
Telecommunications (Data Protection and Privacy) Regulations 1999
Protection of Freedoms Act 2012
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

6. Monitoring, Reviews and Evaluation

The policy will be monitored by the Data Protection Officer. Regular reports to bpha's Senior Management will identify the compliance status for retention, storage and disposal.

7. Associated Documents and Procedures

Data and Document Retention Schedule
Data and Document Retention Protocol
Data Protection Policy
Data Protection Impact Assessments
CCTV Impact Assessment
Special Categories of Personal Data logs

Status	Version – 1
Responsible	Director of IT
Next review date	23 April 2019