Data Protection Policy – G&C001

1. Scope and Objectives

1.1 This policy sets out how data, which is controlled or processed by bpha and its subsidiary companies, ("bpha, the Group, we or us") will be handled by bpha and its employees, ensuring compliance with The General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act (DPA) 2018.

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

1.3 bpha's specific policy objectives are:

- To ensure that bpha is compliant with the provisions of the GDPR and the DPA
- To ensure that staff are aware of and understand the requirements of the GDPR and DPA and the steps that they need to take when handling personal data
- To promote and embed data protection across bpha for all types of data

2. Policy Statement

2.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of its activities bpha will collect, store and process personal data about its customers, employees, suppliers and other third parties, and it is recognised that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

2.2 Employees are obliged to comply with this policy when processing data on bpha's behalf. Any breach of this policy may result in disciplinary action.

3. Definitions

3.1 **Data Subject**: a living, identified or identifiable individual about whom bpha hold personal data. This includes but is not limited to information held about employees, contractors or customers.

3.2 **Data Controllers**: are the people who, or organisations which, determine why and how any personal data is processed. bpha are the data controller in most of the cases where personal data is processed.

3.3 **Data Processors:** include any person or organisation that processes personal data on our behalf and on our instructions, such as external suppliers.

3.4 **Data Owners:** the senior representatives for a department or business unit at bpha's Senior Management Team.

3.5 **Data Stewards:** employees nominated by a Data Owner to conduct Data Steward responsibilities for the data they own.

3.6 **Personal Data**: any information identifying a Data Subject or information relating to a Data Subject that can be identified (directly or indirectly) from that data alone or in combination with other identifiers bpha possess or can reasonably access. Personal data can be factual or an opinion about that person's actions or behaviour.

3.7 **Processing**: any activity that involves use of the data, including obtaining, recording or holding the data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 **Pseudonymisation:** replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information.

3.9 **Employees:** All employees including those on a temporary or fixed term or permanent contracts, workers, work experience, apprentices, agency workers, consultants, contractors, involved residents, volunteers, directors, Board and Committee members.

3.10 **Special Categories of Personal Data:** information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and personal data relating to criminal offences and convictions.

4. Roles and Responsibilities

4.1 The **Board** are responsible for:

- taking ownership of responsibility for Data Protection within bpha, and leading by example
- regularly reviewing bpha's Data Protection Policy
- ensuring the Data Protection Officer is actively supported in their duties and receives continuous training relating to Data Protection

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

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

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

- the security and maintenance of the IT Infrastructure and Cyber Security Landscape
- ensuring bpha have an appointed Data Protection Officer

4.4 **Data Owners** are responsible for:

- overseeing the proper handling of their data or system(s)
- ensuring data accuracy, entry, checking and protection
- ensuring that their areas are compliant with data protection requirements, policies, principles, and procedures
- appointing data stewards

4.5 **Data Stewards** are responsible for:

- day-to-day responsibilities in ensuring compliance in the Data Owner's areas
- responding to Data Protection Officer requests
- modelling bpha's Data Protection behaviours

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

- monitoring and reporting to senior management on data protection policy compliance
- regular auditing of different business units to ensure compliance
- responding to data subject access requests
- reporting data breaches to the Information Commissioner's Office (ICO)
- providing Data Protection advice to staff where requested
- raising high risk data protection impact assessments to ICO
- maintaining records of processing

4.7 The internal **Quality Auditors** are responsible for:

- ensuring that Data Protection features as part of all internal quality audits
- ensuring that all issues identified are rectified as part of the audit regime

4.8 All **employees** are responsible for:

- working in accordance with all corporate policies, procedures and processes related to data protection
- attending regular data protection training
- reporting on any breach of data protection to the DPO as soon as known

5. Policy Details

5.1 DATA PROTECTION PRINCIPLES

5.1.1 Anyone processing personal data must comply with the **eight** enforceable principles of good practice. These provide that personal data must be:

- Processed fairly, lawfully and with transparency.
- Processed in line with what was stated when it was collected
- Adequate, relevant and not excessive for the purpose
- Accurate
- Not kept longer than necessary
- Processed in line with data subjects' rights
- Secure
- Not transferred to people or organisations situated in countries without adequate protection

5.1.2 Fair and Lawful Processing

5.1.2.1 When processing personal data as data controllers, bpha will take appropriate steps to ensure that the requirements of fair and lawful processing are met, including:

- ensuring that all procurement and new projects, policies and systems are assessed using FM-LG008-01 - Data Protection Impact Assessment Form
- ensuring that bpha's externally facing environment including website and applications all have effective and meaningful privacy statements which confirm the purposes for which bpha will process personal data
- confirming that bpha's third party data processors follow our Data Protection policies and schedules
- Only sharing data with third party data processors, where under appropriate contracts or confidentiality agreements, or have the appropriate consent
- only processing personal data for the purposes specifically permitted by the GDPR

5.1.3 Notifying Data Subjects

5.1.3.1 If personal data is collected directly from data subjects, bpha will inform them about:

- the purpose or purposes for which bpha intend to process that personal data
- the types of third parties, if any, with which bpha will share or disclose that personal data to
- the means, if any, with which data subjects can limit the use and disclosure of their personal data

5.1.3.2 If personal data is received about a data subject from other sources, bpha will provide the data subject with this information as soon as possible thereafter.

5.1.4 Adequate, Relevant and Non-Excessive Processing

5.1.4.1 bpha will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

5.1.5 Accurate Data

5.1.5.1 bpha will ensure that personal data held is accurate and kept up to date. bpha will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. All reasonable steps will be taken to destroy or amend inaccurate or out-of-date data.

5.1.6 Timely Processing

5.1.6.1 bpha will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. All reasonable steps will be taken to destroy, or erase from our systems, all data which is no longer required, in line with bpha's Data and Document Retention Schedule.

5.1.7 Processing in Line with Data Subjects Rights

5.1.7.1 All personal data will be processed in line with data subjects' rights, in particular their right to:

- Request access to any data held about them by a data controller
- Prevent the processing of their data for direct-marketing purposes
- Ask to have inaccurate data amended
- Prevent processing that is likely to cause damage or distress to themselves or anyone else
- Where data subjects have exercised their rights in writing, bpha will notify the data subject of our actions

5.1.8 Data Security (Secure by Design)

5.1.8.1 bpha will take appropriate security measures against unlawful or unauthorised processing of data, and against the accidental loss of, or damage to, data.

8.1.8.2 bpha will put in place procedures and technologies to maintain the security of all data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if the data processor agrees, through a binding agreement, to put in place adequate security measures against unlawful or unauthorised processing.

5.1.8.3 bpha will actively incorporate "Secure by Design" principles through Data Protection Impact Assessments and seek to continuously improve both our infrastructure and Cyber Security practices. bpha will maintain data security by protecting the confidentiality, integrity and availability of the personal data.

5.1.8.4 Security procedures include:

- Entry controls - Any individual, without visible and acceptable identification, seen in entry-controlled areas should be challenged and his or her identity verified
- Secure lockable desks and cupboards - Desks and cupboards should be kept locked with the keys removed if they hold confidential information of any kind
- Methods of disposal - Paper documents should be securely disposed of in confidential waste and then destroyed in line with National Archive Guidance. Digital storage devices should be physically destroyed when they are no longer required
- Equipment - Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off or lock their PC or devices when they are left unattended

5.2 TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

5.2.1 bpha will only transfer any personal data it holds to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

- The country to which the personal data is transferred ensures an adequate level of protection for the data subjects' rights and freedoms
- The data subject has given their consent
- The transfer is necessary for one of the reasons set out in the GDPR, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject
- The transfer is legally required on important public interest grounds or for the establishment, exercise, or defence of legal claims
- The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights

5.3 DISCLOSURE AND SHARING OF PERSONAL INFORMATION

4.3.1 bpha may disclose personal data held to third parties, without consent:

- In the event that bpha sell or buy any business or assets, in which case personal data held may be disclosed to the prospective seller or buyer of such business or assets
- If we dispose of some or substantially all of our assets are acquired by a third party, in which case personal data held will be one of the transferred assets
- If bpha are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of its employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of safeguarding, fraud protection and credit risk reduction

5.4 DEALING WITH SUBJECT ACCESS REQUESTS

5.4.1 When receiving telephone enquiries, bpha will only disclose personal data held on our systems if the following condition is met:

- The caller's identity has been validated against a proof of ID to make sure that information is only given to a person who is entitled to it

5.4.2 bpha will suggest that the caller uses bpha's online Subject Access Request form. bpha employees will refer all Subject Access Requests to the DPO.

5.5 EMPLOYEE TRAINING

5.5.1 Data protection e-learning training is a mandatory requirement for all bpha employees and is to be completed within the first 6 months of employment. E-learning training is to be repeated annually for all bpha employees, within Q1-Q4.

5.5.2 bpha employees in customer facing roles will be required to attend additional classroom/Teams data protection training that is tailored to the role requirements. This will include roles in Customer Contact, Housing, Retirement Living, Property Services, Help to Buy, and HR.

5.5.3 Embedded into the training is the expectation that employees will follow these Data Protection behaviours and ground rules:

- **Treat it like it's your own data -** If the data were yours, would you be happy with how bpha are using it? We should work on a need to know basis. Before sharing data consider whether the person "needs to know". This applies internally and externally to bpha
- **Challenging people to control data -** It is important to challenge each other where there is data that is unsecure. Whether it is in the office with computers left unattended and unlocked, or challenging people trying to gain access to the building without a lanyard
- **Questioning the need to hold data -** It is easy to keep data forever, but what staff need to do is question whether we actually need to hold data and for how long
- **Data Conscious -** Data security is everyone's responsibility. Anyone can create and share data that could cause a breach. If data is created it needs to follow bpha's Data and Document Retention Policy
- **Check it. Own it. Secure it. Delete it -** It is your responsibility to check information and to either keep it secure or delete/destroy it appropriately
- **Not afraid to say to need help with data. -** Cyber security and technology are constantly evolving. It is important that everyone is able to say when they need help with data
- **Be a skilled digital employee -** We can work better and more securely by using technology in the right way. It is important to keep learning to become progressively more skilled as a digital employee

5.5.4 Do:

- Lock your workstation or device when it is left unattended
- Challenge people on bpha's premises who are not wearing a lanyard
- Ask why we need to keep data
- Destroy data when it has gone passed our retention guidelines
- Ask Data Protection Officer questions if you are not sure

- Take personal responsibility to prevent data breaches (e.g. personal data lying about).
- Protect personal data like it is your own

5.5.5 Don't:

- Share passwords, even with your team
- Use unsecured document sharing
- Leave printouts with personal information about
- Click on email or web links if you are not 100% sure about them
- Think anything electronically stored is private – if it has someone's name on it, they have a right to see it
- Print items containing personal data unless you have to
- Attach documents to emails. Use links instead (you keep control over where the document can go)

6. Regulatory and Legal Considerations

- The General Data Protection Regulation (EU) 2016/679 (GDPR)
- Data Protection Act 2018
- Section 115 of the Crime and Disorder Act 1998 which allows disclosure of personal information for the purposes of the Act

7. Associated Documents and Procedures

- Data and Document Retention Policy
- Employee Guide
- Bpha website Privacy Notice - https://www.bpha.org.uk/privacy-policy/
- Data Subject Rights Request Procedure
- Data breach reporting procedure

Approved by	Board
Date approved	08/05/2018
Owner	Director of Governance and Compliance
Review date	March 2022