



PRIVACY POLICY

Policy Valid From	9 th August 2021
Last Review date	
Next Review Date	9 th August 2024



Contents

1. Introduction	p1
2. Legislation	p1
3. Data	p2
4. Processing of Personal Data	p3-5
5. Data Sharing	p5-6
6. Data Storage and Security	p6-7
7. Breaches	p7-8
8. Data Protection Officer	p8
9. Data Subject Rights	p9-10
10. Privacy Impact Assessments	p11
11. Archiving, Retention and Destruction of Data	p11

1. Introduction

BHA Enterprise Ltd (hereinafter the “Company”) is committed to ensuring the secure and safe management of data held by the Company in relation to customers, staff and other individuals. The Company’s staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals’ data in accordance with the procedures outlined in this policy and documentation referred to herein.

The Company needs to gather and use certain information about individuals. These can include customers (tenants, factored owners etc.), employees and other individuals that the Company has a relationship with. The Company manages a significant amount of data, from a variety of sources. This data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the GDPR).

This Policy sets out the Company’s duties in processing that data, and the purpose of this Policy is to set out the procedures for the management of such data.

Appendix 1 hereto details the Company’s related policies.

2. Legislation

It is a legal requirement that the Company must collect, handle and store personal information in accordance with the relevant legislation.

The relevant legislation in relation to the processing of data is:

- (a) the UK General Data Protection Regulation (“the GDPR”);

- (b) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications) and
- (c) the Data Protection Act 2018 (“the 2018 Act”)

3. Data

3.1 The Company holds a variety of Data relating to individuals, including customers and employees (also referred to as Data Subjects). Data which can identify Data Subjects is known as Personal Data. The Personal Data held and processed by the Company is detailed within the Fair Processing Notice at Appendix 2 hereto and the Data Protection Addendum of the Terms of and Conditions of Employment which has been provided to all employees.

3.1.1 “Personal Data” is that from which a living individual can be identified either by that data alone, or in conjunction with other data held by the Company.

3.1.2 The Company also holds Personal Data that is sensitive in nature (i.e. relates to or reveals a data subject’s racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation). This is “Special Category Personal Data” or “Sensitive Personal Data”.

4. Processing of Personal Data

4.1 The Company is permitted to process Personal Data on behalf of data subjects provided it is doing so on one of the following grounds:

- Processing with the consent of the data subject (see clause 4.4 hereof);
- Processing is necessary for the performance of a contract between the Company and the data subject or for entering into a contract with the data subject;
- Processing is necessary for the Company's compliance with a legal obligation;
- Processing is necessary to protect the vital interests of the data subject or another person; or
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the Company's official authority;

4.2 Fair Processing Notice

4.2.1 The Company has produced a Fair Processing Notice (FPN) which it is required to provide to all customers whose Personal data is held by the Company. That FPN must be provided to the customer from the outset of processing their Personal Data and they should be advised of the terms of the FPN when it is provided to them.

4.2.2 The Fair Processing Notice at Appendix 2 sets out the Personal Data processed by the Company and the basis for that Processing. This document is provided to all of the Company's customers at the outset of processing their data.

4.3 Employees

4.3.1 Employee Personal Data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by the Company. Details of the data held and processing of that data is contained within the Employee Fair Processing Notice which is provided to prospective Employees at the application stage.

4.3.2 A copy of any employee's Personal Data held by the Company is available upon written request by that employee from the Company's Data Protection Officer (see part 8).

4.4 Consent

Consent as a ground of processing will require to be used from time to time by the Company when processing Personal Data. It should be used by the Company where no other alternative ground for processing is available. In the event that the Company requires to obtain consent to process a Data Subject's Personal Data, it shall obtain that consent in writing. The consent provided by the Data Subject must be freely given and the Data Subject will be required to sign a relevant consent form if willing to consent. Any consent to be obtained by the Company must be for a specific and defined purpose (i.e. general consent cannot be sought). Where consent is being relied on, Data Subjects are free to withhold their consent or withdraw it at any future time.

4.5 Processing of Special Category Personal Data or Sensitive Personal Data

In the event that the Company processes Special Category Personal Data or Sensitive Personal Data, the Company must rely on an additional ground for processing in accordance with one of the special category grounds. These include, but are not restricted to, the following:

- The Data Subject has given explicit consent to the processing of this data for a specified purpose;
- Processing is necessary for carrying out obligations or exercising rights related to employment , social security, or social protection law;
- Processing is necessary for health and social care;
- Processing is necessary to protect the vital interest of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person;
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever court are acting in their judicial capacity; and
- Processing is necessary for reasons of substantial public interest under law.

All the grounds for processing sensitive personal data are set out in Article 9(2) of the GDPR and expanded on in the Data Protection Act 2018.

5. Data Sharing

5.1 The Company shares its data with various third parties for numerous reasons in order that its day to day activities are carried out in accordance with the Company's relevant policies and procedures. In order that the Company can monitor compliance by these third parties with Data Protection laws, the Company may require the third party organisations to enter in to an Agreement with the Company governing the processing of data, security measures to be implemented and responsibility for breaches. This will only apply in situations where the third party is a joint controller.

5.2 Data Sharing

5.2.1 Personal Data is from time to time shared amongst the Company and third parties who require to processthe same Personal Data as the Company. Whilst the Company and third

parties may jointly determine the purposes and means of processing, both the Company and the third party will be processing that data in their individual capacities as data controllers.

- 5.2.2 Where the Company shares in the processing of personal data with a third party organisation (e.g. for processing of the employees' pension), it shall require the third party organisation to enter in to a Data Sharing Agreement with the Company in accordance with the terms of the model Data Sharing Agreement set out in Appendix 3 to this Policy.

5.3 Data Processors

A data processor is a third party entity that processes Personal Data on behalf of the Company, and are frequently engaged if certain of the Company's work is outsourced (e.g. payroll, maintenance and repair works).

5.3.1 A data processor must comply with Data Protection laws. The Company's data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify the Company if a data breach is suffered.

5.3.2 If a data processor wishes to sub-contract their processing, prior written consent of the Company must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

5.3.3 Where the Company contracts with a third party to process personal data held by the Company, it shall require the third party to enter in to a Data Protection Addendum with the Company in accordance with the terms of the model Data Protection Addendum set out in Appendix 4 to this Policy.

6. Data Storage and Security

All Personal Data held by the Company must be stored securely, whether electronically or in hard copy format.

6.1 Paper Storage

If Personal Data is stored on paper it should be kept in a secure place where unauthorised personnel cannot access it. Employees should ensure that no Personal Data is left in a place where unauthorised personnel can access it. When the Personal Data is no longer required it must be disposed of by the employee so as to ensure its secure destruction. If the Personal Data requires to be retained on a physical

file then the employee should ensure that it is affixed to the file which is then stored in accordance with the Company's storage provisions.

6.2 Electronic Storage

Personal Data stored electronically must also be protected from unauthorised use and access. Personal Data should be password protected when being sent internally or externally to the Company's data processors or those with whom the Company has entered in to a Data Sharing Agreement. If Personal Data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be encrypted and stored securely at all times when not being used. Personal Data should not be saved directly to mobile devices and should be stored on designated drives and servers.

7. Breaches

7.1 A data breach can occur at any point when handling Personal Data and the Company has reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach require to be reported externally in accordance with Clause 7.3 hereof.

7.2 Internal Reporting

The Company takes the security of data very seriously and in the unlikely event of a breach will take the following steps:

- As soon as it becomes known the breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the Company's DPO must be notified in writing of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s);
- The Company must seek to contain the breach by whichever means available;

- The DPO must consider whether the breach is one which requires to be reported to the ICO and to the Data Subjects affected and, if appropriate, will do so in accordance with this clause 7;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements

7.3 Reporting to the ICO

The DPO will require to report any breaches which pose a risk to the rights and freedoms of the Data Subjects who are subject of the breach to the Information Commissioner's Office ("ICO") within 72 hours of the breach occurring. The DPO must also consider whether it is appropriate to notify those Data Subjects affected by the breach.

8. Data Protection Officer ("DPO")

8.1. A Data Protection Officer is an individual who has an over-arching responsibility and oversight over compliance by the Company with Data Protection laws. The Company has appointed a Data Protection Officer (DPO). The Company's DPO's details are noted on the Company's website and contained within the Fair Processing Notice at Appendix 1 (Tenant Fair Processing Notice) hereto.

8.2 The DPO will be responsible for:

8.2.1 monitoring the Company's compliance with Data Protection laws and this Policy;

8.2.2 co-operating with and serving as the Company's contact for discussions with the ICO

8.2.3 reporting breaches or suspected breaches to the ICO and data subjects in accordance with Part 7 hereof.

9. Data Subject Rights

9.1 Certain rights are provided to Data Subjects under the GDPR. Data Subjects are entitled to view the Personal Data held about them by the Company, whether in written or electronic form.

9.2 Data Subjects have a right to request a restriction of processing their data, a right to request erasure of their Personal Data, and a right to object to the Company's processing of their data. These rights are notified to the Company's tenants and other customers in the Company's Fair Processing Notice. Such rights are subject to qualification and are not absolute.

9.3 **Subject Access Requests**

Data Subjects are permitted to view their Personal Data held by the Company upon making a request to do so (a Subject Access Request). Upon receipt of a request by a Data Subject, the Company must respond to the Subject Access Request within one month from the day after the date of receipt of the request. The Company:

9.3.1 must provide the Data Subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law.

9.3.2 where the Personal Data comprises data relating to other Data Subjects, must take reasonable steps to obtain consent from those Data Subjects to the disclosure of that personal data to the Data Subject who has made the Subject Access Request, or

9.3.3 where the Company does not hold the Personal Data sought by the Data Subject, must confirm that it does not hold any or that Personal Data sought to the Data Subject as soon as practicably possible, and in any event, not later than one month from the day after the date on which the request was made.

9.4 The Right to Erasure

9.4.1 A Data Subject can exercise their right to erasure (otherwise known as the right to be forgotten) by submitting a request to the Company seeking that the Company erase the Data Subject's Personal Data in its entirety.

9.4.2 Each request received by the Company will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the Data Subject's request in accordance with clause 9.4 and will respond in writing to the request.

9.4.3 Requests for erasure will be considered and responded to by the Company by one month from the day after the date we receive the request.

9.5 The Right to Restrict or Object to Processing

9.5.1 A Data Subject may request that the Company restrict its processing of the Data Subject's Personal Data, or object to the processing of that data.

9.5.1.1 In the event that any direct marketing is undertaken from time to time by the Company, a Data Subject has an absolute right to object to processing of this nature by the Company, and if the Company receives a written request to cease processing for this purpose, then it must do so immediately.

9.5.2 Each request received by the Company will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the Data Subject's request in accordance with clause 9.5 and will respond in writing to the request.

9.6 The Right to Rectification

- 9.6.1 A Data Subject may request the Company to have inaccurate Personal Data rectified. If appropriate, a Data Subject may also request the Company to have incomplete Personal Data completed.
- 9.6.2 Each request received by the Company will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the Data Subject's request in accordance with clause 9.6 and will respond in writing to the request.

10. Privacy Impact Assessments (“PIAs”)

10.1 These are a means of assisting the Company in identifying and reducing the risks that our operations have on personal privacy of Data Subjects.

10.2 The Company shall:

10.2.1 Carry out a PIA before undertaking a project or processing activity which poses a “high risk” to an individual’s privacy. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and accessing Personal Data; and

10.2.2 In carrying out a PIA, include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that it will take to reduce those risks, and details of any security measures that require to be taken to protect the Personal Data.

10.3 The Company will require to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced or mitigated. The DPO will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA they require to notify the DPO within five (5) working days.

11. Archiving, Retention and Destruction of Data

The Company cannot store and retain Personal Data indefinitely. It must ensure that Personal Data is only retained for the period necessary. The Company shall ensure that all Personal Data is archived and destroyed in accordance with the periods specified within its Freedom of Information Policy (Appendix 1).