Privacy Policy

1. Policy Statement

This policy applies to ateb group limited; for our subsidiaries, please see Mill Bay Homes and West Wales Care and Repair for their respective privacy polices

Every day as a business we will receive, use and store personal information about our customers, and colleagues. It is important that this information is handled lawfully and appropriately in line with the requirements of the Data Protection Act 2018 and the General Data Protection Regulation (collectively referred to as the 'Data Protection Requirements').

We take our data protection duties seriously, because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

We will make sure that everyone dealing with your personal information at ateb are familiar and comply with this policy.

2. About This Policy

This policy, and any other documents referred to in it, sets out the basis on which we will process any personal data we collect or process.

The ateb Data Protection Officer is responsible for ensuring compliance with the Data Protection Requirements and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred to the **ateb Data Protection Officer**. Please see section 17 for full contact details or use mydata@atebgroup.co.uk

3. What is Personal Data?

Personal data means data (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession).

Certain types of personal data is classed as **Sensitive personal data,** this includes personal data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about criminal offences or convictions. Sensitive personal data can only be processed under strict conditions, including with the consent of the individual.

4. What is processing?

Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

5. Data Protection Principles

Anyone processing personal data, must ensure that data is:

a. Processed fairly, lawfully and in a transparent manner.
b. Collected for specified, explicit and legitimate purposes and any further processing is completed for a compatible purpose.
c. Adequate, relevant and limited to what is necessary for the intended purposes.
d. Accurate, and where necessary, kept up to date.
e. Kept in a form which permits identification for no longer than necessary for the intended purposes.
f. Processed in line with the individual's rights and 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.
g. Not transferred to people or organisations situated in countries without adequate protection and without firstly having advised the individual.

6. Fair and Lawful Processing

The Data Protection Requirements are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individual.

In accordance with the Data Protection Requirements, we will only process personal data where it is required for a lawful purpose. The lawful purposes include (amongst others): whether the individual has given their **consent**, the processing is necessary for performing a **contract** with the individual, for compliance with a **legal** obligation, or for the **legitimate** interest of the business. When sensitive personal data is being processed, additional conditions must be met.

Please refer to the following documents for more detail on how we will process data:

- Privacy Notice for **job applicants** which can be found on our job application portal, please see our working for us pages on www.atebgroup.co.uk
- Privacy Notice for **customers** which can be found on our website www.atebgroup.co.uk
- Privacy Notice for **employees** can be requested by employees from our HR team
- Privacy Notice for **partners** e.g. suppliers, consultants and contractors etc. can be found on our website www.atebgroup.co.uk

7. Processing for Limited Purposes

In the course of our business, we may collect and process the personal data set out in the **Privacy Policy Schedule.** This data may include data we receive directly (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, location data, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

We will only process personal data for the specific purposes set out in the privacy policy schedule or for any other purposes specifically permitted by the Data Protection Requirements. We will notify those purposes via our Privacy Notices when we first collect the data or as soon as possible thereafter.

8. Notifying Individuals

If we collect personal data directly from an individual, we will inform them about:

a. The purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing.
b. Where we rely upon the legitimate interests of the business to process personal data, the legitimate interests pursued.
c. The types of third parties, if any, with which we will share or disclose that personal data.
d. The fact that the business intends to transfer personal data to a non-EEA country or international organisation and the appropriate and suitable safeguards in place.
e. How individuals can limit our use and disclosure of their personal data.
f. Information about the period that their information will be stored or the criteria used to determine that period.
g. Their right to request from us as the controller access to and rectification or erasure of personal data or restriction of processing.
h. Their right to object to processing and their right to data portability.
i. Their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn.
j. The right to lodge a complaint with the Information Commissioners Office.
k. Other sources where personal data regarding the individual originated from and whether it came from publicly accessible sources.
l. Whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and any consequences of failure to provide the data.
m. The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

9. Adequate, Relevant and Non-excessive Processing

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

10. Accurate Data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

11. Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

12. Processing personal data in line with your rights

We will process all personal data in line with your rights, in particular their right to:

a. Confirmation as to whether or not personal data concerning the individual is being processed.
b. Request access to any data held about them by a data controller (see also *Clause 15 Subject Access Requests*).
c. Request rectification, erasure or restriction on processing of their personal data.
d. Lodge a complaint with a supervisory authority.
e. Data portability.

f. Object to processing including for direct marketing.
g. Not be subject to automated decision making including profiling in certain circumstances.

13. Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

We will put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

a. **Confidentiality** means that only people who are authorised to use the data can access it.
b. **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
c. **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the ateb Group's central computer system instead of individual PCs.

Security procedures include:

a. **Door Entry controls.** Any stranger seen in entry-controlled areas who is not wearing an ateb group visitor badge should be reported to the first available Manager who will take necessary steps to identify that stranger.
b. **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
c. Data minimization. Only collecting sufficient personal data for the specified purposes
d. Pseudonymisation and encryption of data. Replacing any identifying characteristics of sata with a pseudonym, in other words, a value which does not allow the data subject to be directly identified. Ensuring that all personal data sent outside of the Group via electronic means, is encrypted with security measures e.g. password protected
e. Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
f. Equipment. Staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC, or ensure a password protected screen saver is activated as soon as possible when their PC is left unattended. All phones, iPads and tablets will be encrypted/password protected depending on the device.
g. **Transferring Personal Data Outside of the EEA.** We do not transfer data outside of the EEA. If there is a need to pass data outside of the EEA for exceptional reasons we will advise you that the data is being transferred provided that The data subject has given his consent and one of the following conditions applies:

1) The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
2) The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

3) The transfer is legally required on important public interest grounds or for the establishment, exercise or defense of legal claims.
4) 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.

14. Disclosure and Sharing of Personal Data

We may share personal data we hold with any member of the ateb group limited, i.e. Mill Bay Homes, West Wales Care & Repair and Effective Building Solutions subject to their and our privacy policies

We may share personal data with our partners detailed in the Privacy Policy Schedule subject to their and our privacy policies.

15. Subject Access Requests

Individuals must make a formal written request for information we hold about them. When receiving telephone enquiries, we will advise callers to put their request in writing. Where a request is made electronically, we will need to take all reasonable steps to ensure that the person requesting the information is entitled to it.

All request should be forwarded to the **ateb Data Protection Officer.**

16. Training and Development

The Group accepts its responsibility to ensure that managers and colleagues receive adequate learning, development, guidance and support to implement this policy.

17. Changes to this Policy

We reserve the right to change this policy at any time. Where appropriate, we will notify changes by mail or email and on our website.

16. Associated Documents

Documents relating to this procedure are:

- **Privacy Notices for:**
  - PN/1 -Job applicants
  - PN/2 - Customers
  - PN/3 - Employees
  - PN/4 - Partners
- **Privacy Policy Schedule**
- Retention and destruction procedure
- Website and cookie use
- CCTV use
- Electronic data security measures

17. Useful Links

- ateb Data Protection Officer – Julie John
  email: mydata@atebgroup.co.uk
  Tel: 01437 763688
  Or write to Data Protection Officer at ateb group ltd, Meyler House, St Thomas Green, Haverfordwest, Pembrokeshire SA61 1QP

- Information Commissioners Office – https://ico.org.uk/global/contact-us/
  Tel: 0303 123 1113