SA/16 - Data Protection Policy

PN:01

"Our policies embed our culture, establish boundaries and outline our expectations. They have been agreed by our Board(s) as best practice documents for the Group's decision making."

Policy Statement

Every day as a Group we will receive, use and store personal information about our customers, stakeholders and employees. 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.

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.

This policy applies to all ateb Group Limited's, Mill Bay Homes' and West Wales Care & Repair's customers, stakeholders and employees.

Approval Date	Lead Contact	Review Date
27th January 2022	Data Protection Officer	November 2023

Policy Contents

2. Principles

The purpose of this policy and any other documents referred to in it, is to set out how ateb Group Limited, Mill Bay Homes and West Wales Care & Repair handles the personal data of our customers, stakeholders and employees. The policy details the basis upon which we will process any personal data we collect and process in line with the requirements of the Data Protection Act 2018 (**DPA**) and the retained EU law version of the General Data Protection Regulation (**UK GDPR**) (collectively referred to as the '**Data Protection Requirements**').

When we talk about **Personal Data** we mean 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 are classed as **Sensitive Personal Data** (this is also sometimes described as "special category 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, such as with the explicit consent of the individual.

When we talk about **Processing**, we mean any activity that involves use of personal data. Processing 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.

As a Group when processing personal data we comply with the **Data Protection Principles** that personal data will be:

a. Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

b. collected only for specified, explicit and legitimate purposes (Purpose Limitation);

c. adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

d. accurate and where necessary kept up to date (Accuracy);

e. not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);

f. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);

g. not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and

h. made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

1. Lawfulness, Fairness and Transparency

We will only process personal data where it is required for a lawful purpose. The lawful purposes include: the individual has given their consent; the processing is necessary for performing a contract with the individual; for compliance with a legal obligation; to protect the data subject's vital interests; or for the legitimate interests of the business. When sensitive personal data is being processed, additional conditions must be met (see our Privacy Notices for further information).

When we rely on a data subject's consent, which will be in limited circumstances, we ensure that consent is indicated clearly, either by a statement or positive action, such as ticking a box. We respect a data subject's right to withdraw consent at any time and will record and honour any request. If a data subject asks to withdraw their consent but we consider that it is still necessary for us to continue to process their data and we have another lawful basis to do so other than consent, we will explain this to the data subject when their request is made.

2. Purpose Limitation

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 data subject. If we collect personal data directly from an individual, we will inform them of the following (if applicable) through our Privacy Notices and this policy:

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, what are the legitimate interests that are pursued.
c. the types of third parties, if any, with which we will share or disclose that personal data.
d. the fact that the Group 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 Commissioner's Office (ICO).
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 their 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 or such processing for the individual.

The following Privacy Notices detail how we will process your data:

- Privacy Notice - Job Applicants
- Privacy Notice - Employees
- Privacy Notice - Customers
- Privacy Notice - Contractors/Suppliers
  Privacy Notice for Mill Bay Homes
- Privacy Notice for West Wales Care & Repair
- Cookie Policy

As our services improve, the above Privacy Notices may be updated.

3. Data Minimisation

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject. We ensure that excessive data is not collected and will not make unnecessary copies.

Employees must only process personal data when performing their job role requires it, and must not process personal data for any reason unrelated to their job duties.

This applies regardless of whether an employee is working at home, on site or in one of the Group's offices.

When data is no longer needed, we ensure that it is deleted, securely destroyed or anonymised in accordance with our retention guidelines which can be found at appendix 1 to this policy.

4. Accuracy

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.

We respect our customers/stakeholders/employees' rights to check the accuracy of any personal data we hold and request any amendments of the same.

5. Storage Limitation

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. Please see our retention guidelines at appendix 1 for more details.

6. Security, Integrity and Confidentiality

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 or access to personal data transmitted, stored or otherwise processed.

We will put in place policies, processes and technologies to maintain the security of all personal data from the point of 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 they agree to comply with our policies or processes, or if they have/put in place adequate measures themselves.

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 will only be stored on central systems and not on personal devices.

We will ensure that our data security and confidentiality measures are not adversely affected where employees work from home, on site or in a hybrid manner.

We apply the following security measures:

a. Door Entry Controls: Any stranger seen in an entry-controlled area who is not wearing an ateb Group visitor badge is to be reported to the first available manager who will take necessary steps to identify that stranger.
b. use of strong passwords for electronic devices
c. secure lockable desks and cupboards. Desks and cupboards are to be kept locked if they contain confidential information of any kind. (Personal data is always considered confidential.)
d. Homeworking: protocols for the security of data where employees work from home, including: ensuring that employees have a password-protected VPN where they use a shared computer and that passwords are not shared with members of their households; asking employees to be aware of visitors in their home who can overlook their workspaces; asking employees not to take hard copies of documents home, and/or to keep documents secure and return them to the workplace as soon as possible if it is necessary to take documents home on occasion and if documents are no longer needed returning them to the workplace and disposing of them confidently using the confidential waste facilities in place at the office; asking employees to keep their homeworking spaces secure and not to leave company equipment or documents in unlocked premises or in vehicles; and notify the Governance and ICT Teams if their work device is lost/stolen.
e. Data Minimisation: Only collecting sufficient personal data for the specified purposes.
f. Pseudonymisation and encryption of data where possible. Replacing any identifying characteristics of data with a pseudonym, in other words a value which does not allow the data subject to be directly identified.
g. ensuring that all personal data sent outside of the Group via electronic means is encrypted with security measures, e.g., password protected.
h. Methods of Disposal: Paper documents are to be shredded or placed in confidential waste bags to be collected by an approved confidential waste carrier and disposed of securely. Digital storage devices are to be physically destroyed when they are no longer required.
i. Equipment: Employees are to ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC, laptop or tablet, or ensure a password protected screensaver is activated as soon as possible when their equipment is left unattended. All phones, iPads and tablets issued by the Group are to be encrypted/password protected, depending on the device. Employees using their own devices for work purposes need to ensure they use 2 factor verification for emails and MS Teams and are not to save any customer personal data on their systems.
j. not transferring data to people or organisations situated in countries without adequate protection and without firstly having advised the individual.

Employees must comply with all of the above measures at all times, and must not attempt to circumvent any of the administrative, physical or technical safeguards we

implement and maintain in accordance with the Data Protection Requirements. This applies regardless of whether the employee is working in the office, on site or at home. For example, an employee who has a hard copy document stored at home must return it to the office for secure destruction in accordance with paragraph d. above.

Employees must read the above in conjunction with our guidance on IT Security Measures which further details the security measures in place on electronic devices supplied to employees.

7. Transfer Limitation

The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

We do not normally transfer data outside of the UK.

Employees may only transfer personal data outside of the UK if one of the following applies:

a. the UK has issued regulations confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subject's rights and freedoms;

b. appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism;

c. the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or

d. the transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between us and the data subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest.

8. Data Subject's Rights and Requests

We will process all personal data in line with our customers'/stakeholders'/ employees' rights in particular their right to:

a. confirmation as to whether or not personal data concerning them is being processed.
b. request access to any data held about them by a data controller.
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.
h. not have their personal data transferred to people or organisations situated in countries without adequate protection and us without first having advised the individual.
i. be notified of a personal data breach if it is likely to result in a high risk to their rights and freedoms.

A customer/stakeholder/employee wanting to invoke any rights listed above or wanting to make a Subject Access Request (SAR) (request to access personal data), is to make a formal request in writing to the Data Protection Officer.
We will verify the identity of any individual requesting data under any of the rights listed above, for example by requesting photographic ID or speaking to them in person.

Direct Marketing

We obtain our data subjects' prior consent for electronic direct marketing (for example by email, text or automated calls.) The limited exception for our existing customers known as 'soft opt in' allows us to send marketing texts or emails if we have obtained contact details in the course of providing a commercial service to our customers and we are marketing similar products or services and we gave our customers the opportunity to opt out of this when first collecting their details and do so in every message thereafter.

We give our customers the right to object to direct marketing in an intelligible manner and any objections are honoured, recorded and respected. If a customer opts out at any time, their details should be supressed (meaning retaining just enough information to ensure that marketing preferences are respected in the future) as soon as possible.

Data Protection Impact Assessments (DPIAs)

A DPIA must be conducted if we carry out any "high-risk processing activities", such as processing of data of a highly personal nature, or large-scale processing of data; or any major project which involves the use of personal data.

A DPIA must:

a. Describe the nature, scope, context and purpose of the processing activity;
b. Assess necessity, proportionality and compliance measures;
c. Identify and assess any risks posed to individuals; and
d. Identify any additional measures needed to mitigate those risks.

Employees must consult with the DPO if they think that a DPIA may be necessary.

3. Responsibilities

Group

This is a Group Policy which applies to all companies within the Group structure.

Board of Management

The ateb Board of Management, as the parent company within the Group, is responsible for approving the use of this policy.

All subsidiary Boards are responsible for ensuring this policy is being used within their respective companies.

All Line Managers

All line managers are responsible for ensuring that this policy operates effectively within their team which includes the following duties:

- Ensuring their team members understand their responsibilities under this policy
- Ensuring their team members attend training opportunities which include new starter training and refresher training. If any team members require additional training, line managers are to inform the DPO.
- Keeping records of customer consents and withdrawals of consents and sharing the same with the Governance team to include in a central record.
- Ensuring that processes under their control comply with the Data Protection Requirements and principles listed above and protect the processing of personal data.
- Reporting any Subject Access Requests or third party requests and any data protection breaches to the DPO and Governance team as soon as possible
- Informing the DPO of any changes required to the Customer Privacy Notices if a change in their service area leads to a change in the way they process customer personal data.
- Carrying out Data Protection Impact Assessments before the commencement of a project if their work involves implementing major system or business change programmes involving the use of personal data including:
  a. use of new technologies or changing technologies (programmes, systems or processes)
  b. automated processing including profiling
  c. large scale processing of sensitive data
  d. large scale systematic monitoring of a publicly accessible area (CCTV)
- Putting in place adequate Information Sharing Protocols with partners such as statutory bodies when working collaboratively and are required by law to share information with partners (WASPI agreements).
- Ensuring partners or contractors/consultants engaged to provide a service either comply with or have their own data protection policy which meets the

Data Protection Requirements. All contracts should include data protection clauses.

Line managers are to seek the advice of the DPO if they are unsure about how their service area is meeting the Data Protection Principles listed in section 2 of this policy to include direct marketing, or if they need any advice regarding their responsibilities under this policy.

All Employees

All employees are responsible for ensuring they understand this policy and for complying with this policy when processing a customer's personal data and engaging in marketing activities.

Employees' responsibilities under this policy include the following:

- Attending data protection training made available to them and for informing their managers if they have not been offered the same.
- Complying with our Information Security Measures policy and ICT Equipment Usage policy.
- Reporting all data breaches to the DPO and Governance Team as soon as they become aware of a suspected breach so that they can be supported in dealing with the same. There is a duty on the DPO to report reportable breaches to the ICO within 72 hours, so the DPO needs to be aware of any breaches.
- Preserving all evidence relating to a potential breach so that it can be investigated and rectified.
- Reporting any requests by customers to access their data (Subject Access Requests) to the DPO or Governance team so requests can be recorded and dealt with within a reasonable timeframe (no longer than a month).
- Recording and reporting to the DPO or Governance Team any request by customers to implement any of their rights listed in section 2 of this policy.
- Reporting any third party requests for data to the DPO or Governance team for advice as to whether the same can be disclosed.
- Refraining from accessing, disclosing, or processing any personal data other than is necessary to carry out their employee duties.
- Obtaining consent before taking and using photographs of customers/ employees or stakeholders.
- Keeping and maintaining accurate records of any data processing activities carried out in the course of their jobs, including records of data subjects' consents and procedures for obtaining consents.

Stakeholders

All partners, contractors and consultants engaged with the Group are required to comply with this Data Protection policy when processing Group customer data or evidence to the Group how their own policies meet the Data Protection Requirements.

Customers

Customers are responsible for informing the DPO should they have any concerns about the way the Group is using their data. If customers are not satisfied with the response from the DPO they have the right to report a complaint to the Information Commissioner's Office:

ICO Wales
2nd Floor, Churchill House
Churchill Way
Cardiff
CF10 2HH

Customers are asked to inform the Group if their contact details change so we can keep their details accurate.

When making a request to access personal data (Subject Access Request) or when accessing any rights outlined in section 2 of this policy, customers need to put their request in writing for the attention of the DPO. We will aim to record and action any request within 30 days of receipt. We will require identification from customers before providing any personal data.

Key Operational Role Responsibilities

In addition to the responsibilities listed above, the following key role(s) have specific responsibilities for the operational delivery of the policy across the Group:

Data Protection Officer (DPO)

The DPO is responsible for ensuring that there are adequate learning, development, guidance and support opportunities to implement this policy. This includes ensuring there is training available for new starters and annual refresher training for employees.

Any questions about the operation of this policy or the data protection requirements should be directed to the DPO.

Details of the DPO:

Ceri Morgan
ateb Group Limited
Meyler House
St Thomas Green
Havefordwest SA61 1QP

4. Control

The DPO is the lead contact for this policy and for ensuring it remains operationally effective. The DPO will review this policy at least every 2 years.

This policy is a dynamic document and will be amended as required following service reviews or changes to the operating environment.

Board approval will be obtained before any amendments are published and employees will receive refresher training as applicable.

5. Links to other documents

Internal

- Privacy notices for Customers, Employees, Job Applicants and Partners can be found on our website ateb Privacy Notices or Mill Bay Homes Privacy Notice or WWC&R Privacy Notice
- Data Processing Schedule www.atebgroup.co.uk
- Cookies Policy
- Employee Data Protection Procedure
- CCTV Policy
- Guidance on IT Security Measures
- Guidance on Computer Usage, BYOD, data breaches, SAR, third party requests can be found on Yammer or requested from the Governance team.

External

- Data Protection Act 2018/ General Data Protection Regulation
- Information Commissioner's Office ICO Wales

ateb Policy Number: PN01

SA/16 – Data Protection Policy

Additional help

Contact our Governance team quoting the policy reference: PN01

Tel: **01437 763688**
Email: **hello@atebgroup.co.uk**
Facebook **@atebgroup**
Face to Face: **Meyler House, Haverfordwest, SA61 1QP**

Version History

Ver	Date	Changes
1	Nov 2019	Policy approved by Board
2	Jan 2022	Policy reviewed and approved by Board
3		