Data Protection Policy

Introduction

The General Data Protection Regulation (GDPR) of 2016 came into force from 25 May 2018 and replaces all previous Data Protection (DP) laws. Its purpose is to protect the 'rights and freedoms' of living individuals and to ensure that personal data is not processed without their knowledge and is processed with their consent.

The GDPR has been accepted as DP Protection law in the United Kingdom with some extensions - as laid down in UK Data Protection Act 2018. The term 'DP legislation' is used in this policy to denote the collective Data Protection law (of GDPR and UK Act) effective from 25 May 2018. All DP legislation in the UK is regulated by a supervisory authority called the Information Commissioner's Office (ICO).

The DP legislation introduces a number of new concepts and improvements to data subjects' rights. A summary of the regulation is given below:

• gaining explicit consent from data subjects for the use of their personal data;

• processing relevant and adequate personal data, only where this is strictly necessary for legitimate organisational purposes;

• collecting only the minimum personal data required for these purposes and not processing excessive personal information;

• providing clear information to individuals about how their personal data will be used and by whom;

• processing personal information fairly and lawfully;

• maintaining an inventory of the personal data categories that are processed;

• personal data is accurate and, where necessary, up to date;

• retaining personal data only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes;

• keeping all personal data secure;

• only transferring personal data outside the EU in circumstances where it can be adequately protected or where equivalent standards apply;

• the application of the various allowable exemptions;

• the requirement to appoint a Data Protection Officer (DPO) in some circumstances;

• 'special categories' of personal data (previously sensitive personal data) is extended to include biometric and genetic data;

• mandatory reporting of data breaches or data loss in some circumstances;

• enhanced security of personal data, e.g. encryption and anonymisation;

• respecting a subject's access rights, including new provisions such as data portability.

Policy Statement

Bushbury Hill EMB LTD (BHEMB) recognise that communities are made up of people with different needs and values and that those differences are important.

We will promote equality of access for everyone and value their diversity. We will work to eliminate discrimination and, in line with the law, we will treat everyone fairly, regardless of

age, disability, gender, reassignment, marital status including civil partnerships, pregnancy and maternity, race, religion or belief or sexual orientation.

We will ensure that members of all these groups are treated in ways that meet their needs, and that they have equal access to services and/or activities wherever possible.

We will promote their inclusion and challenge discrimination against them.

This policy applies to all employees, board members and others who may be involved in the collection of and processing of personal information on behalf of BHEMB and extends to data whether it is held on paper or by electronic means.

BHEMB is a controller under DP legislation - for personal data processing and makes decisions about how and why it is processed. BHEMB is also a data processor e.g. providing the Housing management services to other landlords.

We are committed to compliance with all DP legislation and the protection of the 'rights and freedoms' of individuals whose information BHEMB collects and processes.

The policy's objectives are to:

- protect the personal data interests of individuals and other key stakeholders by the use of appropriate procedures and controls;
- provide the supporting framework for achieving and maintaining compliance;
- ensure BHEMB meets applicable statutory, regulatory, contractual and/or professional duties.

BHEMB uses personal data information when it carries out many aspects of its day to day business. The organisation is subject to this policy, with some requirements spreading out and imposing responsibilities on partner organisations, e.g. our maintenance contractors. (Typically, they are a Data Processor of personal data that we have collected in our role of Data Controller).

Personal data is all data within our computer systems, including our Housing Management System, Document Management System, email, Word documents, Excel worksheets, plus manual filing systems that refer to a living Data Subject.

Special categories of personal data are considered to be more sensitive and so need more protection. These include racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

This policy applies to all of BHEMB's personal data processing functions, including those performed on personal data and any other personal data processed from any source, relating to:

- tenants & applicants
- clients (any organisation or person(s) to whom we provide a service);
- suppliers and partners (contractors, local authorities and stakeholders);
- Board Members
- Our employees / job applicants.

Any breach of DP legislation or this policy by employees will be dealt with under the Disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

BHEMB's Chief Officer is the designated DPO, who is responsible for reviewing the Data audit register in light of any changes to BHEMB's activities.

Partners and any third party contractors who have access to personnel data will be expected to comply with DP legislation and our DP requirements and agreements detailed in our contracts and SLA's. BHEMB reserve the right to audit compliance with this.

All board members and employees are responsible for BHEMB's policies and procedures.

Data Protection Principles

We are committed to ensuring that we comply with the six data protection principles and the other requirements of GDPR, as follows:

1. Personal data must be processed lawfully, fairly and transparently.
2. Personal data can only be collected for specified, explicit and legitimate purposes.
3. Personal data must be adequate, relevant and limited to the purpose for which the data is processed.
4. Personal data must be accurate and kept up to date.
5. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for the processing purposes.
6. Personal data must be processed in a manner that ensures the appropriate security.

Data Subjects' Rights

Data Processing
Data subjects have the following rights regarding data processing and the data that is recorded about them:

- To make subject access requests to see what information is held on them and who it has been disclosed to.
- Withdraw consent for your data to be used where there is no legitimate reason for that data to be used.
- Amend your data where the data is inaccurate
- Request for your data to be deleted, known as the 'right to be forgotten' where there is no legitimate reason to the data to be get (e.g. Legal / legislative reasons).
- Give explicit consent for your data to be processed in certain circumstances by completing a data permissions form (for example to receive texts on community events).

Complaints
Data subjects who wish to complain about how their personal data is processed can;

- Use BHEMB's complaints policy
- Complain to the ICO (Information Commissioner's Office)

Lawful Basis for Processing Data

BHEMB will collect/ process personal data for the purposes of legitimate interests of allocating / providing and maintaining our properties & where we have a contract with our tenants, we process personal data in order to fulfil it.

Lawful basis is if one of the following conditions is satisfied.

- processing is necessary for the performance of a contract to which the tenant or employee is party or in order to take steps at the request of the tenant or employee prior to entering the contract;
- processing is necessary for compliance with a legal obligation to which BHEMB is subject;
- processing is necessary in order to protect the vital interests of the tenant or employee or of another natural person;
- processing is necessary for the purposes of the legitimate interests pursued by BHEMB or by a third party, except where such interests are overridden by the interests

or fundamental rights and freedoms of the tenant or employee which require protection of personal data, in particular where the data subject is a child.

Special Categories of Personal Data

BHEMB will only collect and process special categories of personal data if there is a legitimate interest and one of the conditions set out below has also been satisfied:

- the data subject has freely given explicit consent to the processing of their personal data for one or more specified purposes;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment law.
- processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent;
- processing relates to personal data which has been made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest. The only categories in this subsection potentially relevant to BHEMB are the administration of justice, (i.e. providing information to the Court or those pursuing proceedings and preventing or detecting unlawful acts);
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment
- processing is necessary for archiving purposes in the public interest or statistical purposes, including the need to complete statutory or regulatory returns in accordance with Legal requirements and Legislation.

It should be noted that for the BHEMB to provide some of our services we need explicit consent from our tenants (e.g. Texting about community events and delivery of local services). The tenant can withdraw consent at any time and exclude themselves from these services.

Disclosure of Data

Exemptions

DP legislation permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (including health, safety and welfare of persons at work);
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, e.g. emergency medical situations.

All requests to provide data for one of these reasons must be supported by appropriate paperwork to justify the decision and all such disclosures must be authorised by the DPO.

Information sharing

BHEMB must ensure that personal data is not disclosed to unauthorised third parties.

All employees should exercise caution when asked to disclose personal data held on an individual to a third-party.

It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of BHEMB's business. We do have certain Information Sharing Agreements in place, e.g. with the Council, police and other agencies using set sharing protocols.

Board members do not have any right to see personal data stored on files, except with the written permission of the individual, or to see any information that would not be disclosed to the individual.

There are situations where information will be withheld, such as where it would identify someone else who has not given consent to the disclosure, unless it can be edited out (redaction).

Safeguarding information
BHEMB actively works to safeguard children, young people and vulnerable adults from harm.

BHEMB has a duty to tell Social Services where an individual's safety is at risk and share information with them, whether reported directly or indirectly to staff.

The types of information that may be shared include names, contact details, information about a person's physical or mental health and relations with others.

BHEMB expects its staff to immediately report any concerns to their line manager and make a safeguarding referral to the appropriate safeguarding authority in Wolverhampton.

In certain limited circumstances DP legislation provides for personal data, even sensitive data, to be shared without the individual knowing about it.

Direct Marketing

BHEMB may use personal data for direct marketing (including to business partnerships) in relation to its activities. This includes email and text, phone calls and direct mailshots. Consent will normally be obtained at the time that personal data is provided by the individual, however consents will be renewed for data that we already hold.

Tenants may withdraw consent at any time by writing to Bushbury Hill EMB, and their details will no longer be used for these purposes.

Employees

Personal data relating to employees is obtained from job applications and whenever data is refreshed through the Business Services Dept or Payroll. The job application form states that the information collected will be strictly confidential and used only for the purposes of personnel and salary administration, or otherwise in connection with BHEMB's business. This includes using data for monitoring purposes and checking email and internet use and checking CCTV for health and safety purposes in the case of an incident. This also appears in contracts of employment. Data will not be kept any longer than is necessary.

BHEMB will comply with the following requests for personal data:

- from agents authorised by the employee, e.g. mortgage requests, references. The employee should confirm in writing that the information is to be released;

• for law enforcement (i.e. by the police for the prevention or detection of crime, assessment or collection of any tax or duty by HM Revenue and Customs or the Child Support or Child Maintenance Agency). Disclosure is only allowed where failure to make the disclosure is likely to prejudice one of these purposes. In all cases the purpose of the request will be obtained in writing;
• if urgently required, for the prevention of injury and damage to health;
• by trade union officials. The employee will be asked to confirm in writing;
• for any other compulsory legal process;
• by specifically identified external sources, e.g. pension administrators, in order to administer internal benefit schemes.

Employees are entitled to see their personal data. Employees are also entitled to know the purposes for which their personal data is intended to be used and the likely recipients (or class of recipients). *(see Staff Privacy Notice for more information)*

The following information is excluded from disclosure:

• parts of references received that identify third-parties and the third-party does not consent to the disclosure and we decide on a balance of interests that it is right to withhold the information;
• personal data used for management forecasting or planning if disclosure is likely to prejudice the conduct of that business or activity only;
• records relating to any negotiations with the employee if disclosure is likely to prejudice those particular negotiations;
• if it involved disclosing information relating to an identifiable third party, unless the third party has consented or it is reasonable to comply without their consent. Failing these options, the data will be edited ('redacted') to protect the identity of third parties. Disclosure will be made if a health record is sought and the third party is a health professional who has compiled or contributed to it. An employee will not be able to prevent processing necessary for the performance of a contract to which the employee is a party. Personal data about an employee given to board members will be edited to remove any third-party information.

Responsibilities

The Board is ultimately responsible for ensuring the BHEMB does not collect information that is not strictly for the purpose for which it is obtained.

The Chief Officer will carry out the role of DPO and along with the senior management team will be responsible for developing and encouraging good information handling practices.

Compliance with DP legislation is the responsibility of all employees who control or process personal data.

Employees are responsible for ensuring their own personal data is accurate and up to date.

Security Breaches

A 'personal data breach' firstly involves a security incident, which leads to compromise of data integrity, availability or confidentiality.

Examples of security incidents include:

- Poor security
  - o cyber security breach by access via a user account;
  - o access to a global email server via an administrator's account;

o ransomware;
o misuse of passwords.

• Data accidentally published
o employee sends email with personal data asking for technical assistance;
o email sent to wrong recipient;
o paper files circulated with too much information included;
o intranet information accidentally goes on website.

• Hacked
o hacking;
o hacking using forged cookies.

• Inside job
o social engineer poses as CEO and emails HR for information on employees;
o employee under notice resets all network servers to factory default settings and disconnects remote backups;
o employee copies protected data onto an external disk;
o malicious employee - passes employee login to hackers;
o malicious employee - publishing HR data to internet.

• Lost/stolen device or media
o stolen laptop/tablet unencrypted;
o decommissioned hard drives not 'scrubbed' but sold on second hand;
o CDs lost in post unencrypted.

Any employee who suspects a data protection breach must report it immediately to their line manager who will liaise with the DPO, it is likely an investigation will need to take place.

Serious breaches will be reported to the ICO within 48 hours of notification of the breach.

Data Audit Log

BHEMB has established this log to record processing activities of personal data, defining:
- purpose of the processing;
- what data is being processed;
- who the data relates to;
- technical and organisational measures taken to secure the data;
- how consent is given and the lawful processing basis used.

Full details are given in the separate Data Audit Log.

Retention and Disposal of Data

BHEMB shall not keep personal data in a form that permits identification of data subjects for longer than it deems necessary (in relation to the purpose(s) for which the data was originally collected).

BHEMB may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data will be set out in the Data Audit Log, along with the criteria used to determine this period including any statutory obligations to retain the data.

Personal data must be disposed of in a way that protects the “rights and freedoms” of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion).

Training

Staff and board members will be required to read and understand this policy as part of their induction.

Staff will be trained on a regular basis on this policy, including about their own rights.

Board members will receive training on GDPR as part of their induction and on a regular basis as needed.

Monitoring and Review

Compliance with this policy will be monitored by the DPO and the policy shall be reviewed every 3 years or upon changes to DP legislation or changes in the practices of the EMB, whichever occurs sooner.