BeneFactors Property Management Limited

General Data Protection Regulations (GDPR)

PRIVACY POLICY

1. INTRODUCTION

BeneFactors Property Management Limited of 7 Queens Gardens, Aberdeen, United Kingdom, AB15 4YD ("we" or "us") is committed to ensuring the secure and safe management of data held by us in relation to clients, staff and other individuals. Our staff members have a responsibility to ensure compliance with the terms of this policy, and to manage the data of individuals in accordance with the procedures outlined in this policy and documentation referred to herein.

As part of the daily operations of our business, we collect and use certain information about individuals. This includes proprietors, employees, contractors, suppliers and other individuals that we have a contractual agreement with. We manage a significant amount of data from a variety of sources. This data contains both "personal data" and "sensitive personal data", which are classed as "special categories of personal data" under the General Data Protection Regulation (GDPR).

This Policy sets out our duties in processing that data, and the purpose of this policy is to outline the procedures for the management of such data.

2. LEGISLATION

It is a legal requirement that we process data correctly, and we 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 **General Data Protection Regulation (EU) 2016/679** ("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) Any legislation that, in respect of the United Kingdom, replaces or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union.

3. DATA

We hold a variety of data relating to individuals, including clients and employees (also referred to as "data subjects") which is known as personal data. The personal data held and processed by us is detailed within the Fair Processing Notice (FPN) within this Policy.

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 us.

We do not hold personal data that could be regarded as sensitive in nature (i.e. data on an individuals' racial or ethnic origin, religious beliefs, political opinions, or relates to their health or sexual orientation).

4. PROCESSING OF PERSONAL DATA

We are permitted to process personal data on behalf of data subjects providing it is doing so on one of the following grounds:

- Processing with the consent of the data subject;
- Processing is necessary for the performance of a contract between us and the data subject, or for entering into a contract with the data subject;
- Processing is necessary for our 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 purposes of legitimate interests.

Fair Processing Notice (FPN)

We have produced a Fair Processing Notice (FPN) which we are required to provide to all clients whose personal data is held by us. The FPN must be provided to the client 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.

Employees

Employee personal data is held and processed by us. Details of the data held and the processing of that data is contained within the employee FPN, which is provided to employees at the same time as their contract of employment.

Consent

Consent as a ground of processing shall be required from time to time by us when processing personal data. It shall be used by us where no other alternative ground for processing is available.

In the event that we require to obtain consent to process a data subject's personal data, we shall obtain that consent in writing. The consent provided by the data subject must be given freely, and the data subject shall be required to sign a consent form if willing to consent.

Any consent to be obtained by us must be for a specific and defined purpose (i.e. general consent cannot be sought).

Where consent is obtained and relied upon, the individual providing that consent has the right to withdraw that consent at any time following it being provided.

Processing of Special Category Personal Data/Sensitive Personal Data

In the event that we process special category personal data or sensitive personal data, we must do so in accordance with one of the following grounds of processing:

- 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 or social security or social protection law;
- 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 courts are acting in their judicial capacity;
- Processing relates to personal data manifestly made public by the individual;
- Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of working capacity of employees, medical diagnosis, the prevention of heath or social care or treatment;
- Processing is necessary for public interest in the area of health;
- Processing is necessary for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes;
- Processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim, and on the condition that it relates to members or former members who have regular contact with the entity; or
- Processing is necessary for reasons of substantial public interest under law.

5. DATA SHARING

We may share our data with various third-party organisations for numerous reasons in order that daily activities are carried out in accordance with our relevant policies and procedures. In order that we can monitor compliance by these third party organisations with data protection laws, we shall require the third party organisations to enter into an agreement with us to govern the processing of data, security measures to be implemented, and responsibility for breaches.

Personal data is from time to time shared amongst us and third party organisations who require to process personal data that we process as well. Both us and the third party organisation shall be processing the data in their individual capacities as data controllers.

Where we share in the processing of personal data with a third party organisation, we shall require the third party to enter into a data sharing agreement with us where the circumstances of the data sharing require such an agreement to be in place.

Data Processors

A data processor is a third party organisation that processes personal data on behalf of us and are frequently engaged if certain parts of our work is outsourced (e.g. payroll, maintenance etc.).

If we choose to appoint a third party organisation to process personal data on our behalf, the following shall be applicable:

a) The data processor must comply with data protection laws. The data processor must ensure that they have appropriate technical security measures in place, maintain records of processing activities and notify us if a data protection breach is suffered.
b) If the data processor wishes to subcontract their processing, our prior written consent must be obtained. Upon subcontracting the processing work, the data processor shall be liable in full for any data protection breach suffered by their subcontractor.
c) Where we contract with a third party to process personal data held by us, it shall require the third party to enter into a data processing agreement with us.

6. DATA STORAGE & SECURITY

All personal data held by us must be stored securely, whether in paper or electronic format.

Paper Storage

If personal data is stored on paper, it should be kept in a secure place where it cannot be accessed by unauthorised personnel. All staff members should ensure that no personal data is left where it could be accessed by unauthorised personnel.

When the personal data is no longer required, it must be disposed of as to ensure its destruction. If the personal data requires to be retained on a physical file, it should be adequately secured within the file (e.g. stapled) and then stored in accordance with our storage provisions.

Electronic Storage

Personal data stored electronically must also be protected from unauthorised use and access. Where possible, personal data should be password protected and encrypted when being sent, both internally and externally.

If personal data is stored on removable media (e.g. CD/DVD disc or USB memory stick) then the removable media must be securely stored at all times when not being used. Where possible, personal data stored on the removable media should be password protected and encrypted.

Personal data should not be saved directly to mobile devices (e.g. phones, tablets or laptops) and stored only be stored on designated drives and servers.

7. BREACHES

A data breach can occur at any point when handling personal data and we have 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 the subject of the breach require to be reported externally to the Information Commissioner's Office (ICO).

Internal Reporting

We take the security of data very seriously. In the unlikely event of a breach, we shall take the following steps:

1. As soon as the breach (or potential breach) has occurred, and in any event no later than 6 hours after it has occurred, the responsible person for data protection matters, must be notified in writing of the breach, how the breach occurred and what the likely impact of the breach is on any data subjects.
2. We must seek to contain the breach by whatever means available.
3. The responsible person for data protection matters must consider whether the breach is one which requires to be reported to the Information Commissioner's Office (ICO) and to notify the data subjects affected.
4. Notify third party organisations (if necessary) in accordance with the terms of any applicable data sharing agreements.

ICO Reporting

The responsible person for data protection matters is required to report any breaches which pose a risk to the rights and freedoms of the data subjects who are the subject of the breach, to the ICO within 72 hours of the breach occurring. The responsible person for data protection matters must also consider whether it is appropriate to notify the data subjects affected by the breach.

8. RESPONSIBLE PERSON FOR DATA PROTECTION MATTERS

We have designated a responsible person for data protection matters whose details are contained within our Fair Processing Notice (FPN). This person is responsible for our compliance with data protection laws.

The responsible person for data protection matters shall be responsible for:

- Monitoring our compliance with data protection laws and this Policy;
- Co-operating with and serving as our contact for discussions with the ICO; and
- Reporting breaches or suspected breaches to the ICO and data subjects as outlined in Section 7 of this Policy.

9. DATA SUBJECT RIGHTS

Certain rights are provided to data subjects under the GDPR:

a) Data subjects are entitled to view the personal data held about them by us, whether in written or electronic format.
b) Data subjects have a variety of rights which include the right to request a restriction of processing their data, a right to be forgotten, and a right to restrict or object to us processing their data. These rights are notified to our clients in our Fair Processing Notice (FPN).

Subject Access Requests

Data subjects are permitted to view their data held by us upon making a written request to do so (known as a "subject access request"). Upon receipt of this request by a data subject, we must respond to this request within one month of the date of receipt of the request.

We:

a) must provide the data subject with an electronic or paper copy of the personal data requested, unless any exemption to the provision of that data applies in law;
b) where the personal data comprises of 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
c) where we do not hold the personal data sought by the data subject, must confirm that we do not hold any personal data sought by the data subject as soon as practicably possible and in any event, not later than one month from the date of receipt of the request.

The Right to be Forgotten

A data subject can exercise their right to be forgotten by submitting a request in writing to us seeking that we erase the data subject's personal data in its entirety.

Each request received by us shall require to be considered on its own merits and legal advice may have to be obtained in relation to such requests before a decision is made.

The responsible person for data protection matters shall have responsibility for accepting or refusing the data subject's request in accordance with this clause and shall respond in writing to any such request.

The Right to Restrict or Object to Processing

A data subject may request that we restrict our processing of the data subject's personal data, or object to the processing of that data.

In the event that any direct marketing is undertaken by us, a data subject has an absolute right to object to processing of this nature by us, and if we receive a written request to cease processing for this purpose, then we must do so immediately.

Each request received by us shall require to be considered on its own merits and legal advice may have to be obtained in relation to such requests before a decision is made.

The responsible person for data protection matters shall have responsibility for accepting or refusing the data subject's request in accordance with this clause and shall respond in writing to any such request.

10. PRIVACY IMPACT ASSESSMENTS (PIAs)

Privacy impact assessments (PIAs) are a means of assisting us in identifying and reducing the risks that our operations have on personal privacy of data subjects.

We shall carry out a PIA before undertaking a project or processing activity which poses a high risk to an individual's privacy.

In carrying out a PIA, we shall 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 we shall take to reduce those risks, and details of any security measures that require to be taken to protect the personal data.

We shall be required to consult the Information Commissioner's Office (ICO) in the event that a PIA identifies a high level of risk which cannot be reduced. The responsible person for data protection matters shall be responsible for such reporting. Where a high level of risk is identified by those carrying out the PIA, they are required to notify the responsible person for data protection matters within 5 working days.

11. ARCHIVING, RETENTION & DESTRUCTION OF DATA

We cannot store and retain personal data indefinitely. We must ensure that personal data is only retained for the period necessary. We shall ensure that all personal data is archived and destroyed timeously, and at the point that we no longer need to retain that personal data in accordance with the periods specified.

The table below sets out retention periods for personal data held and processed by us. Note this table is for guidance only, and that the retention period may vary depending on the individual circumstances relative to the data subject whose personal data is stored.

Record Type	**Retention Period**
Current factored client information	Duration of management contract
Former factored client information	1 year after end of management contract
Debt recovery records/information	3 years
Any other third party records/information	Duration of management contract