Bit4Me Limted

Privacy Policy

May 2018

1. Introduction

This policy sets out Bit4Me Limted ("**the Firm**")'s commitment to data protection, and individual rights and obligations to personal data. Where applicable it draws on the new rules and principles under the General Data Protection Regulation ("**GDPR**")[1].

In the course of the Firm's business, any client[2] personal data held by the Firm is held in a secure and fully protected manner at all times.

Any questions about this policy, or requests for further information, should be directed to the Firm's legal Department.

2. Data protection principles

The Firm processes client personal data in accordance with the following data protection principles:

- The Firm processes personal data lawfully, fairly and in a transparent manner.
- The Firm collects personal data only for specified, explicit and legitimate purposes.
- The Firm processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The Firm keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The Firm keeps personal data only for the period necessary for processing.
- The Firm adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Personal information is collected through the following sources: (i) contractual documents, (ii) Investor questionnaires or forms and (iii) through other information provided by the client in writing, in person, by telephone, electronically or by any other means.

Such information may include, but is not limited to, name, address, nationality, tax identification number, financial and investment qualifications and through investments with the Firm (via the website).

In some cases, the Firm needs to process data to ensure that it is complying with its legal and compliance obligations.

In other cases, the Firm has a legitimate interest in processing personal data before, during and after the end of the contractual relationship. Processing client data allows the company to:

1 REGULATION (EU) 2016/679

2 In this document, the Firm defines 'client' as an investor who is a natural person or, in the case of a corporate entity, its directors, members, employees, shareholders, agents, interns and any other personnel

- Provide products and services to clients such as managing transactions, , meeting tax requirements and performance of any other tasks necessary as part of the ordinary course of the business relationship.
- Market to relevant potential clients or existing clients concerning new products or services via email, telephone, post or in person and ensuring client records are up-to-date for those purposes.
- respond to and defend against legal claims.

The Firm will update client-related personal data promptly if an individual advises that his or her information has changed or is inaccurate. The individual is responsible for updating the Firm of any changes.

Personal data gathered during the business relationship is held in the client's dedicated file (in hard copy or electronic format, or both). The Firm will hold client-related personal data until the client relationship has ended or no longer deemed necessary for the purpose.

The Firm keeps a record of its processing activities in respect of client-related personal data in accordance with the requirements of GDPR.

a. **Individual rights**

As a data subject, clients have a number of rights in relation to their personal data.

b. **Client rights**

Clients have a number of rights in relation to their personal data. They can require the Firm to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the Firm’s legitimate grounds for processing data (where the Firm relies on its legitimate interests as a reason for processing data);
- to process a subject access request;
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the Firm’s legitimate grounds for processing data.

To ask the Firm to take any of these steps, the client should contact the legal department.

3. Impact assessments

Some of the processing that the Firm carries out may result in risks to privacy. Where processing would result in a high risk to client's rights and freedoms, the Firm will carry out a data protection impact assessment to determine the necessity and proportionality of processing.

4. Data breaches

If the Firm discovers that there has been a breach of client-related personal data that poses a risk to the rights and freedoms of clients, it will report it to the Information Commissioner within 72 hours of discovery.

5. International data transfers

The Firm does not sell or rent client information. However, the Firm may share personal information in the following situations:

1. To service providers in connection with the administration and servicing of the client which may include attorneys, accountants, auditors and other professionals.

2. To affiliated companies in order to provide the client with ongoing personal advice and assistance with respect to products and services.

3. To respond to a subpoena or court order, judicial process or request from regulatory authorities;

4. To protect against fraud, unauthorised investments (such as money laundering), claims or other liabilities; and

5. Upon the consent of a client to release such information, including authorisation to disclose such information to persons acting in a fiduciary or representative capacity on behalf of the client.

Where the Firm engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical measures to ensure the security of data.

Client-related personal data may be transferred to countries outside the EEA. Any data transferred outside the EEA will be on the basis of declaration of adequacy of the jurisdiction or any other allowable data transfer strategies.