Parkwalk
investing in innovation

# DATA PROTECTION POLICY – INVESTORS

***Date of publication: May 2018***

## Key Points

- Parkwalk Advisors Ltd (the "**Company**") will collect, store and process personal data about investors. The Company aims to protect all such information, ensuring its confidentiality, integrity and availability.
- The Chief Compliance Officer is responsible for ensuring compliance with the Data Protection Act 2018 (the "**DPA**"), the General Data Protection Regulation ("**GDPR**") and this data protection policy (the "**Policy**").
- The Company will comply with the six data protection principles when processing any personal data.
- The Company will not keep your data for longer than is necessary for the purpose.
- The Company may hold and process sensitive personal data as appropriate. If you wish to know what data is held about you, you must make the request in writing to the Chief Compliance Officer.
- The Company will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.
- The information the Company collects from you shall not be transferred to another entity, country or territory, unless reasonable and appropriate steps have been taken to ensure your information is treated securely and in accordance with this Data Protection Policy.

## Policy in Detail

The DPA was passed to deal with concerns relating to the privacy of individuals resulting from the storing and processing of information and to allow individuals to access information held on them. Together with the GDPR, the DPA will provide a comprehensive legal framework for data protection in the UK as supplemented by the GDPR.

During the course of the Company's activities, it will collect, store and process personal data about investors (or potential investors) who have enquired about or who have made investments through one or more of the Company's funds (the "**Investors**"). The objective of this Data Protection Policy is to protect all such personal information, ensuring its confidentiality, integrity and availability by processing it in accordance with current legislation.

### What Information the Company Holds About You and Why

This Data Protection Policy covers how the Company will control, hold and process personal data (including special category data provided such processing is specifically authorised or required by local laws) relating to all its Investors. The Company is committed to protecting and respecting your privacy.

The Chief Compliance Officer is responsible for ensuring compliance with the DPA/GDPR 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 in the first instance to the Chief Compliance Officer.

**What is Personal Data?**

Personal data is any information relating to an identified natural person or information from which a natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, locating data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Special category personal data includes personal data consisting of information relating to racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life or any alleged or actual criminal offences or proceedings.

**Data Protection Principles**

Anyone processing personal data must comply with the six data protection principles. These provide that:

- processing must be lawful, fair and transparent;
- the purposes of processing must be specified, explicit and legitimate and data should only be used for the specified purpose;
- personal data must be adequate, relevant and not excessive;
- personal data must be accurate and kept up to date;
- personal data must not be kept for longer than is necessary for the purpose; and
- personal data must be processed in a secure manner.

**Information the Company Collects From You and How It Uses It**

The information the Company holds about you includes your name, address, country and date of birth, bank account details, citizenship details and national client identifiers in each country of citizenship and, in some cases, copies of identification documents, including passport or driving licence. The information may be held in hard copy or digital form. Where the data is kept in digital form, it will be stored in restricted folders and may also be password protected. Emailing of such documents will be kept to a minimum, but may be required from time to time, especially between the Company and the Company's custodian (the "**Custodian**") and any nominee used by the Custodian or the Company from time to time (the "**Nominee**") and between the Company and HMRC and the Company and an Investor's IFA.

The Company needs to process personal information for legitimate purposes as part of its day to day business, for management and administrative purposes. The Company also processes personal information for the purposes of complying with its legal and regulatory obligations relating to the detection and prevention of money laundering and complying with obligations in relation to dealing with politically exposed persons.

The Company will only process your personal data for the specific purposes or purposes notified to you or for any other purposes specifically permitted by law. When considering its legitimate interests, the Company will consider interests of individuals along with their reasonable expectations.

The Company will process personal data fairly and lawfully and will only process personal data when necessary for purposes that the Company identifies and of which it makes you aware. The Company will provide such information where the personal data is obtained or, if not practicable to do so at the

time of collection of the personal data, as soon as possible thereafter, unless there is a legitimate reason for not doing so (for example where it is necessary to safeguard national security, the prevention or detection of crime, legal proceedings, tax purposes or where otherwise permitted by law). The Fair Processing Notice, which sets out the purpose for which the Company processes data, is available on the Company's website.

Where the Company processes your special category data, it may seek your consent, though the processing may be necessary to comply with its legal obligations.

If the Company wants to process your personal data for a purpose other than the purpose for which is was originally collected, we will make you aware of such change unless there is a legitimate reason for not doing so. In certain circumstances, such as where the purpose pf processing is substantially different, we will obtain your consent to any such new purposes.

**Accurate Data**

The Company will only retain your personal data where it is adequate, relevant and not excessive in order to properly fulfil the purpose for which that personal data is processed. Data that is inaccurate or out of date will be corrected or destroyed. Please notify us if your personal details change or if you become aware of any inaccuracies in the personal data that the Company holds about you.

**Data Retention**

The Company will not keep your personal data for longer than is necessary for the purpose. This means that data will, so far as is possible, be destroyed or erased from its systems when it is no longer required.

**Your Rights**

Personal data will be processed in line with your rights to:

- request access to any personal data held about you;
- erasure or 'the right to be forgotten', where there is no compelling reason for the continued processing of personal data;
- prevent the processing of your personal data for direct-marketing purposes;
- ask to have inaccurate personal data amended;
- prevent processing that is likely to cause unwarranted substantial damage or distress to you or anyone else;
- object to any decision that significantly affects you being taken solely by a computer or other automated process; and
- data portability which allows personal data to be obtained and reused for your own purposes.

You have the right to request the rectification, deletion or blocking of your personal data which is inaccurate or incomplete and to object, free of charge and at any time on compelling legitimate grounds, to the processing of your personal data (unless the processing is required by law). The Company will rectify, delete, block or cease processing such personal data (as appropriate) in response to the request if we are satisfied there is a legitimate basis for doing so.

Anyone who considers that this Policy has not been followed in respect of personal data about them should raise the matter with the Chief Compliance Officer. For a more detailed summary of your rights under the GDPR, please refer to the appendix.

**Subject Access Request**

If you wish to make a subject access request, you should do so in writing to the Company's Chief Compliance Officer. You are entitled to:

- be informed of whether we hold any process personal data about you;
- be provided with a description of any personal data that we hold about you, the purposes for which any such personal data are being held and the recipients or classes or recipients of whom the information is, or may be, disclosed; and
- a copy of the personal data held by the Company, in an intelligible form.

We will provide this information free of charge unless we consider the request manifestly unfounded or excessive, particularly where the request is repetitive. You will receive a written response within one month of your request unless the request is particularly complex or onerous, in which case we will respond in writing within two months from receiving the request.

**Data Security**

The Company will ensure that appropriate technical, organisational and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data.

A personal data breach occurs when there is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Where a personal data breach occurs, we will immediately take steps to address it, including informing the individual whose data is affected (where there is a high risk to the rights and freedoms of that individuals(s)) and informing the ICO where appropriate. If we notify you of a personal data breach, we will do so in clear and plain language, setting out the details of the breach and how to contact us for more information, any potential consequences of the breach and what measures we will take in order to deal with the breach and prevent it from happening in the future.

You should notify the Chief Compliance Officer immediately if you suspect or become aware of a data loss or data breach.

**Providing Information to Another Country**

The information the Company collects from you shall not be transferred to another entity, country or territory, unless reasonable and appropriate steps have been taken to ensure your information is treated securely and in accordance with this Policy.

Information the Company collects from you may be transferred to, and stored at, a destination outside the European Economic Area ("**EEA**") and may utilise servers not owned or operated by the Company. Such destinations may not have laws which protect your data like the EEA. It may be processed by the Company or by its suppliers operating inside and outside the EEA. Your information shall not be

transferred to a country or entity outside the EEA unless the transfer is made to a country or territory recognised by the EU as having an adequate level of legal protection to protect your rights and freedoms in relation to the processing of your information or is made in compliance with one of the mechanisms recognised by the EU as providing an adequate level of protection when transfers are made to countries or territories lacking an adequate level of legal protection.

**Providing Information to Third Parties**

The Company may also share your personal data with the Custodian, the Nominee, HMRC and your IFA (if applicable) or with any other necessary third parties for the purposes of administering your investment with us and in connection with your and the Company's respective rights and obligations in respect of such relationship and the Company will at all times take adequate measures to safeguard the security of your data.

Your personal data may be stored on non-Company secure physical servers.

**Changes to this Policy**

This Policy is reviewed annually by the Company to ensure it is achieving its stated objectives and to reflect any changes in legislation. Where changes are made to legislation, the Company will amend this Policy in accordance with the changes and outside of the annual review. Any changes that the Company makes to this Policy will appear on the Company's website.

***May 2018***

Parkwalk
investing in innovation

## APPENDIX

**Rights for individuals under the GDPR: A Summary**

| What is the right? | What does this mean? |
|---|---|
| The right to be informed | This covers the obligation to provide fair processing information to individuals (usually through a fair processing notice). It emphasises the need for transparency on how personal data is used. |
| The right of access | Individuals have the right to obtain (via a subject access request):<br>• confirmation that their data is being processed;<br>• access to their personal data.<br>Information must be provided to individuals within one month of receipt of the request (unless the request(s) are complex/numerous, in which case this timeline may be extended by a further two months). |
| The right of rectification | Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.<br>Where a request has been made, a response must be provided within one month. This can be extended by two months where the request is particularly complex. |
| The right to erasure | This right allows individuals to request the deletion or removal of personal data where there is no compelling reason for its continued processing.<br>This right is sometimes known as the right to be forgotten but it does not provide an absolute 'right to be forgotten'. It provides the right to erasure in certain circumstances. |
| The right to restrict processing | Individuals have the right to block the processing of personal data in certain situations. Data processers must restrict processing in the following situations:<br>• where an individual consents, the accuracy of the personal data;<br>• where an individual has objected to the processing and the organisation is considering whether it has legitimate grounds to override the objection;<br>• where processing is unlawful and the individual requests restriction rather than erasure; and<br>• if a data processer no longer needs the data but the individual needs the data to establish, exercise or defend a legal claim. |
| The right to data portability | This right allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily in a safe and secure way. |
| The right to object | Individuals can object to:<br>• processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);<br>• direct marketing (including profiling); and<br>• processing for the purposes of scientific/historical research and statistics. |
| The right in relation to automated decision making and profiling | The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. |