Spire Capital Pty Ltd

Privacy Policy

ACN: 141 096 120

AFSL: 344 365

Date: 23 May 2019

Table of Contents

1. Privacy Policy

1.1 Objectives

Spire Capital Pty Ltd ("**Company**") is subject to the Australian Privacy Principles contained in the Privacy Act 1988 and the Privacy Amendment (Enhancing Privacy Protection) Act 2012, including the **Australian Privacy Principles** The objective of the policy is to describe how the Company complies with the privacy requirements in protecting personal information the Company holds on individuals.

2. Responsibility

2.1 Who must comply with this policy?

All staff are required to comply with this Policy and relevant Privacy Procedures. Employees should specifically comply with the Company's Policy when handling both personal and sensitive information, including that of their fellow employees.

3. Policy

3.1 All staff are required to keep all information confidential.

It is imperative that all information be treated in a sensitive manner as any leak of information may have a material adverse effect on the Company's interests or the best interests of its clients. There is a confidentiality clause within each staff contract.

3.2 Electronic data protection and data security policies and procedures

There are electronic data protection and data security policies and procedures to prevent and detect the occurrence of errors, omissions or unauthorised insertion, alteration or deletion of, or intrusion into, the Company's data processing system (electronic or otherwise) and data (covering all confidential information in the Company's possession, such as clients' personal and financial information and price sensitive information). All client information is held by an independent fund administrator via a secure portal.

3.3 Controls with respect to computer systems

There are controls with respect to access to computer systems, where such devices are used to transmit important information, e.g. funds transfer instructions, settlement instructions and trade confirmations.

3.4 Personal data

The Company shall consider the below areas including, but not limited to, the following when handling client data:

a) the personal data is collected for a lawful purpose to meet its AML/CTF obligations, directly related to the function or activity of the licensed corporation and that the data is adequate but not excessive in relation to that purpose;

b) the personal data is only used for the purposes for which it is collected or a directly related purpose and that the customers give their express consent before their personal data is used for any other purpose;

c) the personal data held is protected against unauthorised or accidental access.

d) where the collection of particular items of personal data is optional, this should be made clear to the customers;

e) any contractual provisions that may have an impact on personal data privacy should be in a font size that is reasonably readable;

f) the person and/or third party to whom a customer's personal data could be transferred should be reasonably specific;

g) personal data transferred to a third party should not be excessive with regard to the purpose for which it is to be used; and

h) ensure that a business partner to whom customers' personal data would be transferred has adequate data privacy protection measures in place.

3.5 The Privacy Officer

The Company must appoint a privacy officer (the Privacy Officer) who is responsible for this Privacy Policy. The Privacy Officer is responsible for:

a) managing data breach notification

b) handling privacy complaints

c) communicating with OAIC

d) reporting to the CEO and the board about privacy matters

e) educating the Company personnel about this Privacy Policy

f) maintaining and updating this Privacy Policy.

4 Overview of the Australian Privacy Principles

4.1 What are the Australian Privacy Principles?

The Australian Privacy Principles (APPs) are 13 general principles that are set out in Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012. The APPs set a minimum standard for the way in which organisations must handle personal and sensitive information. Refer to www.oaic.gov.au for further information.

4.2 The Company must comply with the APPs

Under the Privacy Act, the Company is required to comply with the APPs and any breach of an APP provides a person with the right to complain to the Company and seek an internal investigation or to make a formal complaint to the OAIC. The OAIC also has jurisdiction to investigate breaches of privacy laws at its own initiative, conduct privacy assessments, make determinations and impose civil penalties against organisations which do not comply with privacy laws.

5 Overview of the OAIC

5.1 What is the OAIC?

The OAIC is an independent Australian Government agency established under the Australian Information Commissioner Act 2010. Refer to www.oaic.gov.au for further information,

6 Exceptions to the privacy law obligations

6.1 Limited exceptions

There are several limited exceptions under the Privacy Act to the Company's obligations to comply with the APPs as set out below:

6.2 Circumstances where exceptions apply

a) In each exception circumstance or situation, the Company must **reasonably believe** that the collection, use or disclosure of personal information is **necessary** (i.e. essential) to manage, assist or prevent the relevant circumstance or situation (as applicable).

Exception circumstance/ situation	Criteria
○ serious threat to life, health or safety of an individual	○ there must be a significant danger to the life of an individual or individuals, a potentially life-threatening situation or one that might reasonably result in other serious injury or illness (e.g., harm due a terrorist incident), does not include a threat to an individual's finances or reputation
○ suspected unlawful activity or serious misconduct	○ applies to the Company's internal investigations relating to fraud, dishonesty, deceit, serious misconduct etc. Includes investigations relating to harassment or discrimination
○ missing persons	○ if the use or disclosure of personal information is reasonably necessary to locate a missing person
○ legal or equitable claims	○ if the use or disclosure of personal information is reasonably necessary for the establishment, exercise or defence of an existing legal or equitable claim ○ but does not apply to compel the Company to disclose personal information where such disclosure would be prohibited under another Australia law
○ alternative dispute resolution processes	○ if the use or disclosure is reasonably necessary for a confidential ADR process (i.e. a mediation, conciliation, facilitation, expert, assessment, determination or neutral evaluation) ○ the parties to the dispute must be bound by confidentiality so that the personal information is only disclosed for the confidential ADR process

b) If any of these circumstances exist, the Company is excused from being required to comply with its obligations in respect to personal information as required under applicable privacy legislation. However, the descriptions of the circumstances/situations and criteria above are generic and the decision regarding whether a particular exception is applicable should be made in conjunction with the Privacy Officer by reference to the relevant legislation, guidelines and regulations.

7 General guidelines for handling personal information

Set out below is the Company's approach to the *Australian Privacy Principles* (APPs).

7.1 APP 1 - Open and transparent management of personal information

The Company will ensure personal and sensitive information is managed in an open and transparent way.

Also, the Company will ensure this Policy is regularly reviewed and kept up to date, that this policy is also available on request.

In its **collection** of personal information, the Company will adhere to the following guidelines:

a **privacy collection statement** should always be provided to a person from whom personal information is collected – this is in the form of the Website Privacy Statement (or similar document)

the person will be required to confirm that they have read the Privacy Statement.

In order to satisfy disclosures required in relation to open and transparent management of sensitive and personal obligations, the following information has been provided:

Kinds of personal information collected and held

The Company may collect and hold information such as name, address, telephone number and date of birth. For the purposes of employment, the Company may collect data, such as references from prior employees, employment history, educational qualifications and other information as required.

How personal information is collected and held

Information will be collected via email, mail, telephone etc., the Company may also use other methods as they become available through developments in technology and social media. Information is held in house and externally by the Company service providers including Registry (Locally hosted data-centres, and when an external service provider has overseas based data centres, the Company will ensure that the external service providers adhere to the *Australian Privacy Principles* when handling information overseas.)

Purposes for collecting, holding, using and disclosing personal and sensitive information

Purposes for collecting will be made clear at each stage when the information is collected, which may include – applications, distributions, direct marketing and claims etc.

Accessing and seeking correction of personal information

Please refer to APP 12.

Complaint about a breach of the APPs and how the Company deals with the complaint

Please refer to the Complaints process as outlined in the Company's Complaints Handling Policy.

7.2 AAP 2 - Anonymity and Pseudonymity

a) The Company recognises that it has an obligation to permit individuals to communicate with the Company using a pseudonym or anonymously in certain circumstances.

b) However, the right of an individual to communicate with the Company using a pseudonym or anonymously may apply in circumstances where an individual contacts the Company to merely obtain information about the Company's business and activities. It is the Company's policy in such circumstances to allow individuals to communicate without providing their name, however, such potential customers will be directed to the website for further information.

7.3 AAP 3 - Collection of solicited personal information

The Company must collect personal information which is relevant to the conduct of its equity investments and management business and will only use or disclose that information for the purpose of its business operations.

We aim to use fair and lawful ways to collect information and where reasonably practicable, we attempt to collect personal and sensitive information directly from individuals. When we collect information, we will generally explain to the individual why we are collecting it, who we give it to and how we will use or disclose it. Generally, if applicable we will explain this whether we collect it from the individual or from someone else or these things will be obvious when we collect the information.

The Company may use information collected from our browser and data collection devices such as cookies to improve our operations and facilitate, and improve, the services that clients request. The Company may use information collected from clients to measure interest, customizes experience and enforce the Terms of Use, and determine whether the individual is an accredited investor and have sufficient sophistication, investment experience and wealth to receive information about certain investment options.

The Company uses industry standard practices to protect client privacy, it does not promise, and clients should not expect, that personal information or private communications will always remain private. Accordingly, private communications and other personal information may be disclosed in ways not described in this Privacy Policy. For example (without limiting the foregoing), the Company may be forced to disclose personal information to the government or third parties under certain circumstances, third parties may unlawfully intercept or access transmissions or private communications, or service providers may abuse or misuse personal information that they collect from the website.

7.4 APP 4 – Dealing with unsolicited personal information

The Company is aware of its obligations to destroy or de-identify unsolicited information.

7.5 APP 5 – Notification of the collection of personal information

The Company will notify the individual or ensure they are aware of the collection of personal and sensitive information, and the purpose of its collection, before or as soon as practicable after it is collected.

If the Company collects the personal and sensitive information from someone other than the individual, the company will advise the circumstances of the collection and note the matters. If an individual seeks correction of their personal and sensitive information they are to contact the relevant Entity. Please note the Complaints process as outlined in the Complaints Handling Policy.

a) An independent fund administrator stores personal information on a password protected electronic database on behalf of the Company.

b) Personal information will stay on the database and be retained for the relevant document retention period unless the Company de-identifies it or destroys it earlier in accordance with privacy law requirements.

c) The Company has arrangements which require third party service providers to maintain the security of the information and the Company takes reasonable steps to protect the privacy and security of that information.

7.6 APP 6 - Use and disclosure of personal information

The Company is aware of its obligations with respect to the **use** and **disclosure** of personal information under the APPs, in particular, under APP 6. The Company generally use or disclose personal or sensitive information only for:

a) The primary purpose for which it was collected;

b) A related purpose for which the individual would be reasonably expect; or

c) With consent, unless one of the exceptions applies.

7.7 APP 7 - Direct marketing

The Company is aware of its obligations under APP 7 with respect to direct marketing.

Consent

The Company may only use an individual's personal information for direct marketing where it has obtained the individual's consent or where the individual would reasonably expect the Company to use or disclose the personal information for the purpose of direct marketing, and the Company provides a simple means by which the individual can opt-out of receiving direct marketing communications.

Opting out of direct marketing

The Company will, as part of the collection of personal information from individuals during the investment application process – as provided for in the Privacy Statement – advise individuals that their information will be used for direct marketing purposes, however, they will be given the right to opt-out of receiving such communications.

Unless an individual requests to opt-out or otherwise notifies the Company that it does not wish to receive direct marketing communications, the Company may issue direct marketing communications to individuals in accordance with the Privacy Statement.

All direct marketing communications issued by the Company will provide for a simple mechanism for the recipient to opt-out of receiving future direct marketing communications.

Other direct marketing laws

The Company must also comply with:

Do Not Call Register Act 2006 (DNRC)	Under the DNCR Act, the Company must not make an unsolicited telemarketing call to a person whose name appears on the register. The Company will not engage in widespread unsolicited telemarketing.
Spam Act 2003 (Spam Act)	Under the Spam Act, the Company must not send an electronic commercial message unless the message includes a functional and legitimate 'unsubscribe' facility, including an electronic address the recipient can use to tell the Company they do not wish to receive messages. The Company will ensure that all of its email direct marketing messages include such an unsubscribe facility.

7.8 APP 8 – Cross-border disclosure of personal information

Where the Company stores personal information with an external service provider, the Company acknowledges that this is a 'use' of that personal information but it is not a 'disclosure' of that personal information. Accordingly, APP 8 (regarding cross border disclosure) does not apply to the Company.

7.9 APP 9 – Government related identifiers

The Company intends to adopt, use or disclose Commonwealth Government identifiers only where permitted to do so.

Medicare and pension numbers are identifiers, it does not include ARBN and Australian Business Numbers or Tax File Numbers.

If the Company is required to collect a government identifier in providing services to individuals, it will only use this number internally as an identifier, to identify the individual.

As a rule, the Company will not disclose a government identifier to any other person, except as required by law or if the disclosure is requested in writing by the individual to whom the identifier pertains.

7.10 APP 10 - Quality of personal information

We aim to keep Personal and Sensitive information we hold relevant, accurate, current and complete having regard to the use or disclosure requirements.

We will take reasonable steps to ensure that the Personal and Sensitive information that is collected, used and disclosed by us is relevant, accurate, up-to-date, and complete.

If you contact us for a correction, we will firstly confirm your identification, so that we can confidently correct Personal and Sensitive information held

7.11 APP 11 - Security of personal information

The Company will generally take reasonable steps to protect personal and sensitive information from misuse, interference, loss and unauthorised access, changes or disclosure. The Company will destroy or permanently de-identify it when the information is no longer needed for its purpose for which the information was collected, or the Company is no longer required to hold the information under an Australian Law, or a court/tribunal order to retain the information.

7.12 APP 12 - Accessing personal information

The Company has obligations to provide individuals with access to personal information that the Company has on record that the individual is not able to access themselves.

7.13 APP13 - Correction of personal information

The Company has obligations to take reasonable steps to correct personal information and to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.

The Company's obligations to correct information – no request

If the Company becomes aware that personal information it holds is not accurate, subject to applicable laws (for example, its obligations not to "tip off" under the AML/ CTF legislation – see the AML/ CTF Policy), it will rectify the information and it will notify the individual concerned.

The Company's obligations to correct information - request

If the Company receives a request from an individual to correct their personal information:

a) **response time**: the Company must respond in a timely manner

b) **refusal to correct**: if the Company does not consider that it should correct the information, the Company must set out in writing its reasons for refusing to correct the personal information and must notify the individual of the complaint mechanisms available.

c) **associate a statement**: The Company is required to take reasonable steps to associate a statement by the person if they believe that their personal information is incorrect with the person's personal information to make it apparent to users of that information, and

d) **no charge**: the Company is not permitted to charge an individual for dealing with a request for correction or associating a statement.

8 Data breach reporting

8.1 Notifiable Data Breaches Scheme

Notification of serious ('eligible') data breaches are now mandatory under Australian privacy laws. The Notifiable Data Breaches (NDB) scheme under Part IIIC of the Privacy Act 1988 (Privacy Act) establishes requirements for entities in responding to data breaches. Entities have data breach notification obligations when a data breach is likely to result in **serious harm** to any individuals whose personal information is involved in the breach.

The Australian Parliament passed the Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB scheme) on 13 February 2017. The NDB scheme applies to all entities covered by the Australian Privacy Principles (APPs) from 22 February 2018 with clear obligations to report eligible data breaches.

This notification must include recommendations about the steps that the individual should take in response to the eligible data breach.

The Company is required to take all reasonable steps to ensure an assessment is completed within 30 days maximum, after the day the Company became aware of the data breach. If an eligible data breach is confirmed, the Company must provide a statement to each of the

individuals whose data was breached or who are at risk, including details of the breach and recommendations of the steps individuals should take. A copy of the statement must also be provided to the Office of the Australian Information Commissioner (OAIC).

8.2 Privacy Officer's role

The Company adheres to the principle that each data breach should be evaluated on a case-by-case basis and the Company's Privacy Officer will make a decision on an appropriate action to take according to an assessment of the risks and responsibilities of the particular circumstances.

8.3 Circumstances of data breach

The Company recognises that data breaches may occur as a result of the following circumstances:

a) lost or stolen laptops, removable storage devices, or paper records containing personal information

b) hard disc drives and other digital storage media (integrated in other devices, for example, multifunction printers, or otherwise) being disposed of or returned to equipment lessors without contents first being erased

c) databases containing personal information being 'hacked' into or otherwise illegally accessed by individuals outside of the Company

d) employees accessing or disclosing personal information outside the requirements or authorisation of their employment

e) the Company's accidentally providing personal information to the wrong person, or

f) an individual deceiving the Company into improperly releasing the personal information of another person.

8.4 Data breach response plan

The Company responds to data breaches by reference to a Data Breach Response Plan which has been issued to meet the requirements of the Notifiable Data Breaches Scheme.

9 Handling complaints

Refer to the Complaints Handling Policy which outlines the complaint handling procedures for the Company.

10 Monitoring compliance

Any instances of non-compliance by Company staff members will be reviewed by the Privacy Officer. Where instances of non-compliance with the Policy have been identified, the Privacy Officer in conjunction with the board, is responsible for determining or recommending appropriate remedial action and reporting obligations.

Intentional or reckless non-compliance with this Policy is not tolerated by the Privacy Officer and the board. Depending on the nature and extent of non-compliance, remedial action could be taken.

Staff should be aware that breaches of this Policy are taken very seriously.

10.1 Record keeping

The Privacy Officer is responsible for ensuring that the following information in relation to this Policy is retained for a period of at least 7 years:

a) all approved versions of this Policy (including details of their approval)

b) any relevant registers which relate to the Policy

c) records evidencing compliance or non-compliance with the Policy

d) details of any reviews undertaken by the Privacy Officer

e) evidence of induction and ongoing training, and

f) any other documentation relevant to the implementation of and compliance with the Policy.

10.2 Review and updating the Policy

The Privacy Officer will review the contents of this Policy at least annually to ensure it remains current and relevant to the operations of the Company. As part of the review, the Board in conjunction with the Privacy Officer will also ensure that any related policies or procedures are reviewed in consultation with representatives and personnel. The Privacy Officer will report the findings to the Board once the review has been finalised.

10.3 Further information

If you need further information regarding this Policy and how it is implemented, you should contact the Privacy Officer.

10.4 What's next?

The Privacy Officer will be responsible for updating this policy for new legislative requirements and training staff in respect of these requirements.