**finnCap Ltd**

**Client Data Protection Policy**

# Introduction

* 1. In the course of our acting for you, we may receive information relating to you, your directors, shareholders, beneficial owners, employees, agents, associates and family members. In this Policy, we refer to this information as "personal data".
  2. This Policy sets out the basis on which we will process this personal data. Please read the Policy carefully to understand our practices regarding personal data and how we will use it.

# About FINNCAP LTD

* 1. The data controller in respect of personal data is finnCap Ltd, a limited liability company registered in England and Wales under number 06198898. Our registered office is at 60 New Broad Street, London, EC2M 1JJ.
  2. finnCap Ltd is registered with the Information Commissioner’s Office under registration number Z9884968.
  3. finnCap Ltd is authorised and regulated by the Financial Conduct Authority (“FCA”).
  4. References in this Policy to “finnCap”, “we”, “our” and “us” are references to finnCap Ltd.

# contacting us

* 1. Mark Tubby has been appointed as the firm’s Privacy Manager.
  2. If you have any questions about this policy or your information, or to exercise any of your rights as described in this policy or under applicable data protection laws, you can contact us as follows:

The Privacy Manager

finnCap Ltd, 60 New Broad Street, London, EC2M 1JJ

By email: [PrivacyManager@finncap.com](mailto:PrivacyManager@finncap.com)

By telephone: +44 (0)20 7220 0500

# DATA PROTECTION PRINCIPLES

* 1. Anyone processing personal data must comply with the principles of processing personal data as follows:
     1. Lawfulness, fairness and transparency – data must be processed lawfully, fairly and in a transparent manner.
     2. Purpose limitation - data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
     3. Data minimisation - data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
     4. Accuracy - data must be accurate and, where necessary, kept up to date.
     5. Storage limitation - data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
     6. Integrity and confidentiality - data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage by using appropriate technical or organisational measures.
  2. This Policy describes the personal data that we collect, and explains how we comply with these principles.

# INFORMATION WE COLLECT

* 1. We collect the personal data as necessary to enable us to carry out your instructions, to manage and operate our business and to comply with our legal and regulatory obligations.
  2. The personal data that we collect includes, but is not limited to, the following:
  + your name;
  + home and business address;
  + contact details (such as telephone numbers and email address);
  + date of birth;
  + gender;
  + marital status;
  + copies of passport, national identity card, driving licence, utility bills, bank statements and similar documents;
  + business and professional qualifications and experience;
  + immigration status and work permits;
  + financial details;
  + other personal data contained in correspondence and documents which you may provide to us;
  + data from building access controls; and
  + information we obtain from our IT and communications monitoring.
  1. If you do not provide any personal data that we ask for and that we need to enable us to carry out your instructions, it may delay or prevent us from providing our services to you.
  2. Where the personal data relates to your directors, shareholders, beneficial owners, employees, agents, associates or family members you confirm that you are authorised to provide this personal data to us. It is not always reasonably practicable for us to provide to these individuals the information set out in this Policy. Accordingly, where appropriate, you are responsible for providing this information to any such individuals.

# how your information is collected

* 1. We collect most of this information from you directly. However, we also collect information:
     1. from publicly accessible sources, e.g. Companies House;
     2. directly from a third party, e.g. client due diligence providers;
     3. from a third party with your consent, e.g.:
  + your bank or building society, another financial institution or advisor;
  + consultants and other professionals you may engage; and
  + your employer, professional body or pension administrators.
    1. via our website - we use cookies on our website (for more information on cookies, please see our cookie policy at <https://www.finncap.com/cookie-policy>.
    2. via our information technology systems, e.g.:
  + online matter management and document management systems;
  + building access control systems and reception logs.

# how and why we use your information

* 1. Our use of your personal data is subject to your instructions, data protection laws and our professional duty of confidentiality.
  2. We will only process your personal data if we have a legal basis for doing so, including where:
     1. processing is necessary for the performance of our contractual engagement with you: this relates to all personal data we reasonably need to process to carry out your instructions and provide our services to you;
     2. processing is necessary for compliance with a legal obligation to which we are subject: this relates to our legal obligations in relation to, for example, anti-money laundering; and
     3. processing is necessary for the purposes of the legitimate interests pursued by us or by a third party, except where such interests are overridden by your interests or fundamental rights and freedoms: this relates to our processing for marketing purposes, for our management, accounting and administration purposes and for data security.
  3. The table below further explains the purposes for which finnCap will use your personal data (excluding sensitive personal data) and our legal basis for doing so:

|  |  |
| --- | --- |
| **Purposes for which we will process the information** | **Legal Basis for the processing** |
| To provide investment banking or brokerage services to you. | For the performance of our contract with you or to take steps at your request before entering into a contract.  To comply with our legal and regulatory obligations. |
| To carry out associated administration and accounting in connection with the services and other processing necessary to comply with our professional, legal and regulatory obligations. | For the performance of our contract with you or to take steps at your request before entering into a contract.  To comply with our legal and regulatory obligations. |
| To comply with our anti-money laundering requirements. | To comply with our legal and regulatory obligations. |
| To comply with our internal business policies. | It is in our legitimate interests or those of a third party to adhere to our own internal procedures so that we can deliver an efficient service to you. We consider this use to be necessary for our legitimate interests and proportionate. |
| For operational reasons, such as improving efficiency, training and quality control. | It is in our legitimate interests to be as efficient as we can so we deliver the best service for you. |
| To prevent unauthorised access and modifications to our systems. | It is in our legitimate interests to prevent and detect criminal activity that could be damaging for finnCap and for you.  To comply with our legal and regulatory obligations |
| For updating client records. | For the performance of our contract with you or to take steps at your request before entering into a contract.  To comply with our legal and regulatory obligations. |
| For marketing our services. | It is in our legitimate interests to market our services. We consider this use to be proportionate and will not be prejudicial or detrimental to you. |
| To carry out credit reference checks. | **It is in our legitimate interests to carry out credit control and to ensure our clients are likely to be able to pay for our services.** |
| External audits and quality checks, e.g. the audit of our accounts. | **It is in our legitimate interests to carry out quality checks and audit to ensure that we operate at the highest standards.**  **To comply with our legal and regulatory obligations.** |

* 1. Where we request personal data to identify you for compliance with anti-money laundering regulations, we shall process such information only for the purposes of preventing money laundering or terrorist financing, or as otherwise set out in this Policy or permitted by law.
  2. Where we rely on legitimate interests as a lawful basis, we will carry out a balancing test to ensure that your interests, rights and freedoms do not override our legitimate interests. Where you provide consent, you can withdraw your consent at any time and free of charge, but without affecting the lawfulness of processing based on consent before its withdrawal. You can update your details or change your privacy preferences by contacting our Privacy Manager as provided in “Contacting us” above.
  3. finnCap will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will notify you in a timely manner and we will explain the legal basis which allows us to do so.
  4. finnCap acts as a data controller in relation to the processing of personal data as set in this Policy. However, in some circumstances we may process personal data on your behalf as a data processor for the purposes of data protection laws. Where we process any personal data on your behalf as your data processor, the terms set out in our data processing addendum, a copy of which is available on request from our Privacy Manager, shall apply.

# SPECIAL CATEGORIES OF (“SENSITIVE”) PERSONAL DATA

* 1. You may also supply us with, or we may receive, special categories of (or “sensitive”) personal data. This is defined by data protection laws to include personal data revealing a person’s racial or ethnic origin, religious or philosophical beliefs, or data concerning health.
  2. We process these special categories of personal data on the basis of one or more of the following:
     1. where you have given explicit consent to the processing of the personal data for one or more specified purposes;
     2. where the processing relates to personal data which is manifestly made public by you;
     3. where the processing is necessary for the establishment, exercise or defence of legal claims;
     4. where the processing is necessary for reasons of substantial public interest, in accordance with applicable law. Such reasons include where the processing is necessary:
        1. for the purposes of the prevention or detection of an unlawful act or for preventing fraud;
        2. for the provision of confidential advice.

# DATA RELATING TO CRIMINAL CONVICTIONS & OFFENCES

* 1. We collect and store personal data relating to criminal convictions and offences (including the alleged commission of offences) only where necessary for the purposes of:
     1. the prevention or detection of an unlawful act and is necessary for reasons of substantial public interest;
     2. providing or obtaining legal advice; or
     3. establishing, exercising or defending legal rights.

# marketing

* 1. We use your personal data to notify you by email, telephone, post or SMS about important financial developments and services which we think you may find valuable, for sending you newsletters, invitations to seminars and similar marketing.
  2. In this connection we may disclose personal data to third parties providing marketing services to us, or with whom we are conducting joint marketing exercises.
  3. You have the right to opt out of receiving direct marketing communications from us at any time by:
  + contacting our Privacy Manager using the contact details set out above; or
  + using the “unsubscribe” link in emails
  + sending us an email.

# Email and TELEPHONE monitoring

* 1. Email which you send to us or which we send to you may be monitored by finnCap to ensure compliance with professional standards and our internal compliance policies. We may also record telephone calls as evidence of your orders or instructions. Monitoring is not continuous or routine, but may be undertaken on the instruction of a director where there are reasonable grounds for doing so.

# Third party processors

* 1. Our information technology systems are operated by finnCap but some data processing is carried out on our behalf by a third party (see section 13 on *Disclosure of Personal data*). Details regarding these third party data processors can be obtained from our Privacy Manager whose details are given above.
  2. Where processing of personal data is carried out by a third party data processor on our behalf we endeavour to ensure that appropriate security measures are in place to prevent unauthorised

# Disclosure of personal data

* 1. Personal data will be retained by us and will not be shared, transferred or otherwise disclosed to any third party, save as set out in this Policy.
  2. If we are working with other professional advisers in relation to any matter handled by us on your behalf then, unless you instruct us otherwise, we shall assume that we may disclose your information to them.
  3. We disclose and share personal data:
     1. with finnCap directors, staff, agents and consultants based in the UK;
     2. to other professional advisers and third parties in accordance with your instructions;
     3. to our professional indemnity insurers, and our auditors, or risk managers who we or they may appoint;
     4. third party processors, service providers, representatives and agents that we use to make our business more efficient, including for our **[**IT services, data storage/back-up and marketing**]**;
     5. if we, acting in good faith, consider disclosure to be required by law or the rules of any applicable governmental, regulatory or professional body including the FCA.
  4. Certain laws (for example, those relating to money laundering and tax fraud) give power to authorities such as the police or the tax authorities to inspect clients’ information and take copies of documents. It is possible that, at any time, we may be requested by those authorities to provide them with access to your information in connection with the work we have done for you. If this happens, we will comply with the request only to the extent that we are bound by law and, in so far as it is allowed, we will notify you of the request or provision of information.
  5. We may transfer personal data to a successor firm or company which acquires the business carried on by us. If this happens, we shall ensure that you are notified of the transfer and we shall secure a commitment from the firm or company to which we transfer personal data to comply with applicable data protection laws.

# Your rights

* 1. *Access to your information and updating your information*
     1. You have the right to access information which we hold about you. If you so request, we shall provide you with a copy of your personal data which we are processing (“*subject access request*”). We may refuse to comply with a subject access request if the request is manifestly unfounded or excessive or repetitive in nature.
     2. You also have the right to receive your personal data in a structured and commonly used format so that it can be transferred to another data controller ("*data portability*"). This right only applies where your personal data is processed by us with your consent or for the performance of a contract and when processing is carried out by automated means.
     3. We want to make sure that your personal data is accurate and up to date. You have the right to have inaccurate personal data rectified, or completed if it is incomplete. We may refuse to comply with a request for rectification if the request is manifestly unfounded or excessive or repetitive.
  2. *Right to object*
     1. You have the right to object at any time to our processing of your personal data for direct marketing purposes.
  3. *Where we process your information based on our legitimate interests*
     1. You also have the right to object, on grounds relating to your particular situation, at any time to processing of your personal data which is based on our legitimate interests. Where you object on this ground, we shall no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims.
  4. *Your other rights*
     1. You also have the following rights under data protection laws to request that we rectify your personal data which is inaccurate or incomplete.
     2. In certain circumstances, you have the right to:
        1. request the erasure of your personal data erasure (“*right to be forgotten*”);
        2. restrict the processing of your personal data to processing to which you have given your consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of others.
  5. Please note that the above rights are not absolute, and we may be entitled to refuse requests, wholly or partly, where exceptions under applicable law apply. We may refuse a request for erasure, for example, where the processing is necessary to comply with a legal obligation or necessary for the establishment, exercise or defence of legal claims. We may refuse to comply with a request for restriction if the request is manifestly unfounded or excessive or repetitive in nature.

# EXERCISING YOUR RIGHTS

* 1. You can exercise any of your rights as described in this policy and under data protection laws by contacting our Privacy Manager.
  2. Save as described in this policy or provided under applicable data protection laws, there is no charge for the exercise of your legal rights. However, if your requests are manifestly unfounded or excessive, in particular because of their repetitive character, we may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or taking the action requested; or (b) refuse to act on the request.
  3. Where we have reasonable doubts concerning the identity of the person making the request, we may request additional information necessary to confirm your identity.

# SECURITY OF YOUR INFORMATION

* 1. We store your information in hard copy and in electronic format. We use industry standard technical and organisational measures to protect information from the point of collection to the point of destruction. For example:
     1. Hard copy information files are restricted to authorised individuals
     2. We use, as appropriate, encryption, firewalls, access controls, policies and other procedures to protect information from unauthorised access.
     3. Where appropriate, we use pseudonymisation and / or encryption to protect your information.
  2. We will only transfer personal data to a third party if it agrees to comply with those procedures and policies, or if it puts in place adequate measures itself.
  3. Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted over the internet.

# INTERNATIONAL TRANSFERS

* 1. To deliver services to you, it is sometimes necessary for us to transfer and store your personal data outside the European Economic Area (“**EEA**”) as follows:
     1. with our service providers located outside the EEA;
     2. if you are based outside the EEA;
     3. where there is an international aspect to the services which we have been instructed on.
  2. Where personal data is transferred to and stored outside the EEA, we take steps to provide appropriate safeguards to protect your personal data, including:
     1. transferring your personal data to a country, territory, sector or international organisation which the European Commission has determined ensures an adequate level of protection, as permitted under Article 45(1) GDPR;
     2. entering into standard contractual clauses approved by the European Commission, obliging recipients to protect your personal data as permitted under Article 46(2)(c) GDPR;
     3. under the EU-U.S. Privacy Shield Framework which enables U.S. business to self-certify as a means of complying with EU data protection laws;
  3. In the absence of an adequacy decision or of appropriate safeguards as referenced in 17.2 above, we will only transfer personal data to a third country where one of the following applies (as permitted under Article 49 GDPR)):
     1. the transfer is necessary for the performance of our contractual engagement with you;
     2. the transfer is necessary for the establishment, exercise or defence of legal claims; or
     3. you have provided explicit consent to the transfer.
  4. If you want further information on the specific mechanism used by us when transferring your personal data out of the EEA, please contact our Privacy Manager using the details set out above.

# HOW LONG WE KEEP YOUR INFORMATION

* 1. Personal data received by us will only be retained for as long as necessary to fulfil our engagement. Following the end of our engagement we will retain your information:
     1. to enable us to respond to any queries, complaints or claims made by you or on your behalf; and
     2. to the extent permitted for legal, regulatory, fraud and other financial crime prevention and legitimate business purposes.
  2. After this period, when it is no longer necessary to retain your personal data, we will securely delete or anonymise it in accordance with our Data Retention Policy. Further details regarding our data retention policy can be obtained from our Data Protection Officer whose details are given above.

# COMPLAINTS

* 1. Our Privacy Manager can be contacted at PrivacyManager@finncap.com to whom complaints should be addressed in the first instance.
  2. You have the right to make a complaint at any time with a supervisory authority, in particular in the EU (or EEA) state where you work, normally live or where any alleged infringement of data protection laws occurred. The supervisory authority in the UK is the Information Commissioner’s Office (“ICO”) who can be contacted at https://ico.org.uk/ or telephone on 0303 123 1113.

# Changes to this Policy

* 1. We may change this Policy from time to time. The current version of this Policy will always be available from us in hard copy or on our website. We will post a prominent notice on our website to notify you of any significant changes to this Policy or update you by other appropriate means.
  2. This Policy was last updated on **25 May 2018.**