



MORRISON&CO

PRIVACY POLICY

1 Privacy Policy

H.R.L. Morrison & Co Group LP and all its related entities (**MCO**, our **Group**, **we**, **us** or **our**) are committed to protecting individuals' privacy in accordance with applicable privacy and data protection laws, including the General Data Protection Regulation or "**GDPR**" under the respective EU and UK laws, and the Swiss Federal Act on Data Protection or "**FADP**". MCO is committed to taking our data protection and privacy responsibilities and the security of your personal information seriously.

Important information about MCO:

The entity responsible for your personal information (known as the "controller" under some data protection laws), will be the member of our Group that originally collects information from or about you and/or determines the purposes and means of the processing of such personal information.

If you are located in New Zealand, then your information will be collected by H.R.L. Morrison & Co Limited of 5 Market Lane, Te Aro, Wellington (**MCO NZ**) and will be held by MCO NZ.

You can find out more about our Group by contacting us using the information in the contact us section.

This Privacy Policy describes our current policies and practices in relation to the processing (which includes: the collection, storage, handling, use and disclosure) of personal information. MCO may process personal information relating to the following types of individuals :

- visitors to our websites;
- contractors, consultants and staff;
- contacts at investors, advisors and market participants; and
- certain specified individuals of investors as required by the know-your-customer obligations in the Anti-Money Laundering and Counter-Terrorism Financing laws and regulations.

This Privacy Policy informs you of:

- How is personal information collected?;
- Notification of collection of personal information;
- What personal information we collect, how we use it and the lawful basis for our processing;
- What if you don't provide information to us?;
- How do we hold and protect personal information;
- How we share and disclose personal information within MCO, with regulators and other third parties Our websites and how we use cookies;
- Legal rights available to help manage your privacy, including your right to object to processing (some rights apply only to UK and EU residents);
- What happens if you want to complain?

We may amend this Privacy Policy from time to time, including to reflect changes in the law or our information handling practices and the way we operate our business. Where we make changes that are minor or that relate to security requirements, we will notify you of those changes on our website. If we make more substantive changes that might impact on how your personal information is collected, used or shared by us, then we will give you reasonable prior notice, and where required by applicable law, we will seek your consent in relation to the same. This Privacy Policy was last updated in November 2021.

2 How is personal information collected?

We will only collect personal information from you where we are permitted to do so under applicable laws, that is where the information is reasonably necessary for one or more of our functions or activities and where the information is collected for a lawful purpose connected with one or more of our functions or activities, and the collection is necessary for that purpose.

We endeavour to collect personal information by lawful and fair means. MCO will collect personal information directly from you (for example, where you provide the information to us). In limited circumstances (where legally permitted), we may collect personal information from other sources, including:

- information we receive from any third party authorised by the individual to be his/her representative;

- an individual's employer or a company of which the individual is an officer (where authorised, if applicable);
- publicly available sources of information or databases subscribed to by MCO;
- information received by MCO on subscription agreements and other forms (where authorised, if applicable);
- information about transactions with affiliates in our Group (where authorised, if applicable); and
- information received when you use our websites (see paragraph 9 for details).

3 Notification of collection of personal information

We will take reasonable steps to notify you if we collect, or have collected, your personal information (unless this is not required or an exception applies under the applicable law). Where required under applicable laws, we will also obtain your consent prior to our collection of your personal data.

We will make you aware of the name and contact details of the organisation collecting and holding the information. Where the collection is authorised or required by law we will identify that law, whether or not the supply of information is voluntary or mandatory, and the consequences (if any) of not providing all or part of the requested information.

The notification may also include details about the purposes for which we are collecting the information, the legal basis we rely on to process the personal information and the types of entities we may share the information with (including, where applicable, whether the information is disclosed to overseas recipients and, if practicable, their location). We will also refer you to the information in this Privacy Policy about how you may exercise your privacy rights including the right to access and correct the information we hold about you, and how to complain to a data protection authority.

4 What personal information we collect, how we use it, why we use it and the lawful bases for our processing

When we provide services related to investor relations, client relationship development and arranging investments, we ask you for the information we need to provide the relevant services. The types of personal information that we collect will depend on the particular dealings we have with you.

The kinds of personal information we may collect, and hold includes (but is not limited to):

- personal identifiers, such as name, address, age, contact details and date of birth;
- information relating to an individual's profession, including job title and work contact details;
- information that is required or authorised by law such as, if you are in New Zealand, the *Anti-Money Laundering and Countering Financing of Terrorism Act 2009*, and if you are in Australia, the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth);
- individuals' opinions about our products, services and/or staff; and
- personal information included in any enquiries individuals make using any online or offline means to contact us.

The purposes for which MCO collects personal information are as follows:

- servicing clients (e.g. for administrative purposes, to communicate with you, to provide ongoing information, to respond to queries, for relationship development, and to provide any other requested services);
- providing financial services to wholesale clients, including:
 - advising in relation to securities, interests in managed investment schemes (excluding investor directed portfolio services), basic deposit products and deposit products other than basic deposit products, derivatives and foreign exchange contracts;
 - dealing in financial products by arranging for another person to issue, apply for, acquire, vary or dispose of securities, interests in managed investment schemes (excluding investor directed portfolio services), basic deposit products and deposit products other than basic deposit products, derivatives and foreign exchange contracts; and
 - providing custodial or depository services other than investor directed portfolio services;
- managing the security and control of information and communication systems, including our websites;
- complying with our obligations to detect, investigate, report and seek to prevent fraud and anti-money laundering in accordance with applicable anti-money laundering and counter-terrorism financing laws and regulations; and

- complying with other regulatory and legal obligations and to prevent fraud and identity theft.

We also collect, use and disclose information about job applicants for purposes connected with assessing their suitability for employment or engagement including alerting them to future possibilities they may be interested in (upon, where required by applicable law, their prior consent).

Where employees and contractors are employed/engaged we collect, use and disclose information about them (including information obtained during the application stage) related to their employment/engagement and for related purposes, including payroll/ payment services. This may include disclosure to and use by third party agents or contractors providing services to us.

We will not use or disclose your personal information for any other purpose, or collect sensitive information, without an appropriate legal basis (which may be your consent or one of the applicable legal bases identified below), unless we are required to do so by law. Before using your personal information, we will take such reasonable steps (if any) in the circumstances to ensure that the information is accurate, up to date, complete, relevant, and not misleading.

We may also assign you a unique identifier (e.g. a number or reference connected to you) if that is necessary to enable us to carry out our functions efficiently, and where we have taken all reasonable steps to ensure your identity is clearly established.

If you are located in the UK or EU, the legal basis on which we process personal information will be one or more of the following:

- the processing is necessary for the **performance of a contract** to which you are a party or in order to take steps at your request prior to entering into a contract. For example, the terms of use of our websites;
- the processing is necessary for compliance with a **legal obligation** to which we are subject to. For example, in order to set you or your employer up as a client, we are obliged to carry out certain know-your-customer checks to prevent money laundering and fraudulent activities. This will involve the collection and verification of personal information of relevant members of an organisation, such as directors, trustees and beneficiaries as relevant; or
- the processing is necessary for the purposes of the **legitimate interests** pursued by us or by a third party (e.g. your employer), namely to provide our products and services to our customers, except where such interests are overridden by your interests or fundamental rights and freedoms. Where relevant to website use, our legitimate interest is to use personal information in the aggregate to understand how

our services and the resources provided on our websites are used. We collect this information to help improve our services. Please see Attachment A for further details on the legitimate interests we have for processing personal information. In exceptional circumstances, we may rely on your consent.

If you would like to find out more about the legal basis for which we process personal information, please contact us.

5 What if you don't provide information to us?

In most cases, the provision of your personal data is not required by a statutory or contractual obligation. However, in some circumstances, if you do not provide us with some or all of the information that we ask for, we may not be able to provide certain services to you or a customer with whom you are associated.

For job applicants, your application may not be progressed if you do not provide some or all of the information that we ask for.

6 How do we hold and protect personal information?

We strive to maintain the relevance, reliability, accuracy, completeness and currency of the personal information we hold and to protect its privacy and security. We keep personal information only for as long as is reasonably necessary for the purpose for which it was collected, to comply with any applicable legal requirements, or if we reasonably believe there is a prospect of litigation relating to your personal information or dealings. After it is no longer required, personal information is either destroyed or de-identified. We hold personal information in both electronic and hard copy formats. We ensure that personal information is safe by implementing physical, electronic and procedural safeguards (including up-to-date security software), to prevent unauthorised access, use, modification, disclosure or other misuse.

We hold the personal information we collect on secured servers which are locked at all times. Access is only permitted to authorised persons who need that information for the uses outlined under paragraph 4. Any party that receives personal information will also use it only for those purposes and will not be permitted to use it for any other purpose. If other parties provide support services to MCO, we require them to implement appropriate safeguards to protect the privacy of the information we provide to them, and to prevent its unauthorised use or disclosure. This may include requiring the execution of data processing and non-disclosure agreements to ensure the confidentiality and security of personal information.

As the security of information depends in part on the security of the device you use to communicate with us and the security you use to protect user IDs and passwords, please take appropriate measures to protect this information.

7 How we share and disclose personal information within MCO, with regulators and other third parties

We do not sell, trade, or rent personal information to others. We may disclose personal information in accordance with the relevant law to, for example:

- other entities within our Group, where such disclosure is necessary to provide our services to our clients, to manage our contractual relationships or to manage our business;
- contractors and third-party service providers, where the disclosure is for one of the purposes connected with the collection of the information or is directly related to the purposes for which the information was obtained;
- professional advisors, including accountants, auditors, lawyers and advisors in connection with the administration, processing and servicing of client transactions;
- other persons where required or provided for by applicable laws;
- government agencies, enforcement agencies or regulators as authorised or required by applicable law, and to comply with requests of law enforcement, regulatory and other governmental agencies including tax institutions;
- anyone authorised by you to receive, use or access your personal information; and/or
- if, in the future, we sell or transfer some or all of our business or assets to a third party, we may disclose information to a potential or actual third party purchaser of our business or assets and professional advisors providing services to us.

The contractors and service providers who may receive your personal information include those handling mailings on our behalf, external data storage and computer system maintenance or payment gateway systems. However, we will take all reasonable steps to ensure that they protect the personal information in the same way that we do, including by imposing contractual obligations on contractors and service providers selected by us to implement measures to maintain the security, confidentiality and integrity of personal information.

8 Why we may transfer personal information outside a jurisdiction

As MCO is a global business, we may transfer, store or disclose your information in any country where our Group has an office (as set out at www.hrlmorrison.com) or otherwise conducts

business, but the most likely disclosure will be to recipients located in New Zealand, Australia, the United Kingdom, Hong Kong, Switzerland, the United States and the Asia-Pacific region.

We will take appropriate steps to ensure that transfers of personal information are in accordance with applicable laws and carefully managed to protect your privacy rights and interests. We will take appropriate steps to ensure that transfers are limited to countries which are recognised as providing an adequate or comparable level of legal protection to that in your country of residence or where we can be satisfied that alternative arrangements are in place to protect your privacy rights. To this end, for example:

- we ensure that transfers of personal information collected within the UK, the EU or Switzerland, and transferred outside of the UK, the EU or Switzerland, respectively within our Group companies will be covered by an agreement entered into by members of the Group (an intra-group agreement) which contractually obliges each member to ensure that personal information receives an adequate and consistent level of protection in accordance with applicable data protection laws wherever it is transferred within our Group;
- where we are legally required to do so, any other transfers of personal information collected within the UK, the EU or Switzerland, and transferred to parties located outside UK, the EU or Switzerland, respectively, will be made pursuant to the UK government approved, the European Commission approved, or the Swiss Federal Data Protection and Information Commissioner approved standard contractual clauses (as applicable), or other legally acceptable mechanisms that ensure an adequate level of protection; and
- where we receive requests for information from law enforcement or regulators, we carefully validate these requests before any personal information is disclosed.

If you live in the European Union (**EU**) or the United Kingdom (**UK**) you have a right to contact us for more information about the third countries to which your data is transferred and the safeguards we have put in place (including a copy of relevant contractual commitments such as Standard Contractual Clauses or Binding Corporate Rules) to ensure the adequate protection of your personal information when this is transferred as mentioned above. However, please note that we are not required to share details of safeguards where sharing such details would affect our commercial position, or create a security risk.

9 Our websites and how we use cookies

Individuals are always free to contact us with a question or problem related to their interactions with our websites. The standard business practice of MCO is to retain any communications

from visitors to our websites to help us improve our services. MCO is not responsible for the privacy policies of any third party websites that may be linked to our websites.

In order to collect anonymous data and improve your experience on our websites we may use "cookies". Cookies are small pieces of information which are sent to a website visitor's browser and stored on their computer's hard drive. Sometimes cookies identify users where the website requires information to be retained from one page to the next. This is purely to increase the functionality of the site, to allow the visitor's computer to interact effectively and to enhance security. Cookies by themselves cannot be used to discover the identity of the user. Cookies do not damage a website visitor's computer and you can set your browser to notify you when receiving a cookie so that you can decide if you want to accept it. Cookies also help allow the website to recognise your computer when returning in the future.

To the extent required by applicable law, we will obtain your consent before deploying non-essential cookies when you visit our websites.

We will not identify a particular website visitor's browsing activities, except where we are required or authorised to do so by law.

10 Legal rights available to help manage your privacy, including your right to object to processing

You have certain rights in relation to the information that we hold about you. In accordance with and subject to applicable law, upon receipt of a request from you and sufficient information to allow us to identify you, we will confirm whether we hold your personal information and disclose to you the personal information you have requested that we hold. We will also correct, amend or delete any personal information that we agree (or consider on our own initiative) is inaccurate, irrelevant, out of date, incomplete or misleading. In accordance with applicable law, we may charge you for reasonable expenses incurred in providing access to or correcting your personal information. In New Zealand, where we provide access to information requested, we will advise you that you may request the correction of that information. In Singapore, where we provide access to information requested, you may also request information on how we have used and disclosed your personal information in the 12 months prior to your request.

Anyone who wishes to receive confirmation that we hold their personal information, access or correct their personal information should please contact us, using the information below and provide specific details as to the type of personal information you are seeking to access or the specific changes that need to be made. We will respond to requests for confirmation, access or correction as soon as practicably possible after receiving the request, and within the timeframe required by the relevant legislation.

In addition to the above, if you are an **EU or UK resident**, you have the following rights in relation to your personal information. These rights are however, subject to certain exemptions, and in some cases dependent upon the processing activity we are undertaking:

You can object to the use of your personal information, which has our legitimate interests as its legal basis including for the purpose of marketing. See below for more information on this right.

Click on the links below to learn more about each right you may have:

- to access personal information
- to correct personal information
- to erase personal information
- to restrict the processing of your personal information
- to transfer your personal information
- **to object to the processing of personal information**
- to obtain a copy of personal information safeguards used for transfers outside your jurisdiction
- to lodge a complaint with your local supervisory authority

If you wish to exercise any of the above mentioned rights, we may ask you for additional information to confirm your identity and for security purposes, in particular before disclosing personal information to you.

You can exercise your rights by contacting us at: compliance@hrlmorrison.com. Subject to legal and other permissible considerations, we will make every reasonable effort to honour your request promptly or inform you if we require further information in order to fulfil your request.

Please note that the aforementioned rights may be limited under the applicable data protection laws.

We may not always be able to fully address your request, for example if it would impact the duty of confidentiality we owe to others, or if we are legally entitled to deal with the request in a different way.

- Right to access personal information
You have a right to obtain from us confirmation as to whether or not personal information concerning is being processed, and where that is the case, to request that we provide you with a copy of your personal information that we hold. You have the right to be informed of: (a) the source of your personal information; (b) the purposes, legal basis and methods of processing; (c) the controller's identity; and (d) the entities or categories of entities to whom your personal information may be transferred.

You have a right to obtain a copy of the personal information undergoing processing. For further copies requested by you, we may charge a reasonable fee based on administrative costs.

- Right to correction

You have the right to request that we correct an error or omission in the personal information about you that we hold, and send the corrected personal information to every other recipients to which that personal information was disclosed by us.

- Right to erasure (right to be forgotten)

You can also request that we erase your personal information in limited circumstances where:

- it is no longer needed for the purposes for which it was collected; or
- you have withdrawn your consent (where the data processing was based on consent); or
- following a successful right to object (see right to object); or
- it has been processed unlawfully; or
- to comply with a legal obligation to which we are subject.

We are not required to comply with your request to erase personal information if the processing of your personal information is necessary:

- for compliance with a legal obligation; or

for the establishment, exercise or defence of legal claims.

- Right to restrict the processing of your personal information

You can ask us to restrict the processing of your personal information. In this case, the respective personal information will be marked and only processed for certain restricted purposes. This right can only be exercised where:

- the accuracy of the personal information is contested, to allow us to verify its accuracy; or
- the processing is unlawful, but you do not want it erased; or

- it is no longer needed for the purposes for which it was collected, but you still need it to establish, exercise or defend legal claims; or
- you have exercised the right to object, and verification of overriding grounds is pending.

We can continue to use your personal information following a request for restriction, where:

- we have your consent; or
 - we require the personal information to establish, exercise or defend legal claims; or
 - to protect the rights of another natural or legal person.
- Right to transfer your personal information
You can ask us to provide your personal information to you in a structured, commonly used, machine-readable format, or you can ask to have it transferred directly to another entity, but in each case only where:
 - the processing is based on your consent or on the performance of a contract with you; and

the processing is carried out by automated means.

- Right to object to the processing of your personal information
You can object to any processing of your personal information which has our legitimate interests as its legal basis, if you believe your fundamental rights and freedoms outweigh our legitimate interests.

If you raise an objection, we have an opportunity to demonstrate that we have compelling legitimate interests which override your rights and freedoms.

The right to object does not exist, in particular, if the processing of your personal information is necessary to take steps prior to entering into a contract or to perform a contract already entered into.

- Right to withdraw consent
If you have given us your consent for the processing of your personal information, you have the right to withdraw your consent at any time. Note that this will not affect the lawfulness of any processing of your personal information that we have carried out based on the consent before its withdrawal.

- Right to obtain a copy of personal information safeguards used for transfers outside your jurisdiction

You can ask to obtain a copy of, or reference to, the safeguards under which your personal information is transferred outside of the UK or the European Union.

We may redact data transfer agreements to protect commercial terms.

- Right to lodge a complaint with your local supervisory authority

You have a right to lodge a complaint with your local data protection authority if you have concerns about how we are processing your personal information.

We ask that you please attempt to resolve any issues with us first, although you have a right to contact your data protection authority at any time.

To exercise your rights, please [contact us](#) using the contact information below.

We reserve the right to charge a fee where permitted by law, for instance if your request is manifestly unfounded or excessive.

In this situation, MCO will provide an estimate of how much this service will cost and request the individual's agreement to the cost before proceeding. In some circumstances we may require payment of the whole or part of the charge in advance.

In some limited cases, we may need to refuse access to an individual's personal information (or aspects of it) or refuse a request for correction, including if there are legal, regulatory or administrative reasons to deny access to the requested information or giving access would reveal evaluative information that we are permitted to protect. We will advise the individual as soon as possible after their request is received if this is the case and provide a written statement explaining the reasons for our refusal. We will also provide information about the mechanisms available to make a complaint about the refusal, including in New Zealand the right to seek an investigation and review of the refusal through making a complaint to the Privacy Commissioner

Where an individual has requested we make a correction and we do not agree, we will, if requested by the individual, take reasonable steps to attach to the information in such a way that will make the statement apparent to users of the information a statement of the correction sought but not made.

For EU individuals, personal Information is held until the end of the services provided by MCO and its authorised processors and a subsequent period of ten (10) years thereafter where necessary to comply with applicable laws and regulations or to establish, exercise or defend

actual or potential legal claims, subject to the applicable statutes of limitation, unless a longer period is required by applicable laws. In any case, personal information will not be held for longer than necessary with regard to the purposes described in this Privacy Policy, subject always to applicable local legal minimum retention periods.

11 What happens if you want to complain?

If you have any concerns about whether we have complied with applicable data protection laws or this Privacy Policy when collecting, storing or handling personal information, or for more information about this Privacy Policy, please write to our Compliance Manager at (compliance@hrlmorrison.com).

We will consider the complaint through our internal complaints resolution process and will generally try to acknowledge receipt of your complaint within 7 days of you making a complaint, and respond in writing with a decision as soon as practicable after the complaint is made.

If you are not satisfied with the result of the complaint to us, or if that process is not otherwise appropriate or applicable, you can refer the complaint your local data protection authority:

Australia: Office of the Australian Information Commissioner

GPO Box 5218

Sydney NSW 2001

Telephone: 1300 363 992

Facsimile: 02 9284 9666

Email: enquiries@oaic.gov.au

Online privacy complaint form: www.oaic.gov.au

New Zealand: Office of the Privacy Commissioner

PO Box 10094

Wellington 6143

Telephone: 0800 803 909

Email: enquiries@privacy.org.nz

Online privacy complaint form: www.privacy.org.nz

United Kingdom: Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5A

Telephone: 0303 123 1113

Online privacy complaint: <https://ico.org.uk/make-a-complaint/>

Luxembourg: Commission Nationale pour la Protection des Données (CNPD)

Service des réclamations

15 Bd du Jazz

L-4370 Belvaux

Grand Duchy of Luxembourg

Telephone: +352 26 10 60 1

Online privacy complaint: <https://cnpd.public.lu/en/particuliers/faire-valoir/formulaire-plainte.html>

Singapore: Personal Data Protection Commission

10 Pasir Panjang Road

#03-01 Mapletree Business City

Singapore 117438

Online complaint form: <https://www.pdpc.gov.sg/complaints-and-reviews/report-a-personal-data-protection-concern/personal-data-protection-complaint>

Switzerland: Federal Data Protection and Information Commissioner

Feldeggweg 1

CH-3003 Bern

Telephone: +41 (0)58 462 43 95

Facsimile: +41 (0)58 465 99 96

Online privacy complaint form: <https://www.edoeb.admin.ch/edoeb/de/home/der-edoeb/kontakt/kontaktformular.html>

12 Attachment A – Further information on our legal bases for using personal information

What we use your information for	Further details	Legal basis for using personal information	Explanation for legitimate interests' legal basis
<p>Name and contact details of contact person</p> <p><u>We collect the name and contact details of the employee within your entity in order to obtain and provide information in relation to the services we provide to you.</u></p>	<p>We may also collect information of persons who sign contracts on behalf of the entity engaging us.</p>	<p>Performance of a Contract</p>	<p>Not applicable</p>
<p>Meta Data</p> <p>Some meta data, such as your IP address, will be used to enable you to access our website. The metadata will also be used to improve the quality of our services and our website by analysing user behaviour.</p>	<p>We will collect referral page, date and time of access, type of web browser, IP-address, geographic location, operating system and interface, language and version of browser software.</p>	<p>Legitimate interests</p>	<p>Our legitimate interest is to use personal information in the aggregate to understand how website users use our services and the resources provided on our website and use this information to improve our services.</p>
<p>Contract Notification Information</p> <p>We will use this information to send you updates and relevant notices in relation to the contract and to manage the contractual relationship we have with your employer.</p>	<p>As an employee of our clients, we will collect personal information related to your role.</p> <p>Such personal information will include your name, job title, employer, work email address, work telephone number, office address.</p>	<p>Legitimate interests</p>	<p>Our legitimate interest for use of this information is for effective customer management and service communications.</p>
<p>Direct Communications</p> <p>We will use your personal information to respond to you and to improve our services.</p>	<p>We will collect information such as your name, address, telephone number, profession and job details.</p>	<p>Legitimate Interests</p>	<p>Our legitimate interest is to use personal information to respond to you and to improve our services.</p>
<p>Performing AML Checks</p> <p>We will use your personal information to assess your or</p>	<p>Through know-your-customer checks, AML screening and other identity checks to meet our obligations under any contract</p>	<p>Legal Obligation</p>	<p>Not applicable</p>

<p>your employer's suitability as a client, to comply with our legal obligations, to detect, investigate, report and seek to prevent fraud and anti-money laundering.</p>	<p>we have with you. We may conduct credit and fraud checks on you or your employer's business and certain officers of your employer's business, such as directors.</p>		
---	---	--	--