



# IFM Privacy Statement

This is the external privacy statement of IFM Investors Pty Ltd and its subsidiaries, branches, local employing entities, associates, and affiliated companies (hereafter “IFM Group”, “IFM”, “us,” “our”, or “we”). This external privacy statement outlines how IFM may collect, store, use and disclose Personal Data<sup>1</sup> depending on the type of engagement you may have with us. You will be issued with a specific privacy notice depending on the type of engagement you have with us.

## Contact Details

IFM serves as the ‘data controller’ for the Personal Data it holds and manages, determining both the purposes and means of its processing.

You can contact us by either email or post.

Our postal address in Australia is:

Attn: Privacy Officer  
Address: Level 33, 50 Lonsdale Street  
Melbourne VIC 3000  
Australia

The postal addresses for all IFM office locations can be found [here](#).

Alternatively, you can contact us via email at [dataprotection@ifminvestors.com](mailto:dataprotection@ifminvestors.com).

## What Personal Data do we collect?

While we are required to collect certain types of Personal Data to fulfil our legal obligations, we aim to limit the collection of your Personal Data to only what is necessary to provide the products and services you need.

Depending on the type of engagement with IFM, we may collect the following types of Personal Data. This may include sensitive personal information (or ‘special category Personal Data’) that we may use with your consent; this type of data is *italicised* below.

Categories of Personal Data	Examples
Personal details	Full name; age/date of birth; birth gender; marital status; staff number/other identifier; job title; organisation; residency and work permit status; nationality/citizenship/place of birth; <i>racial or ethnic origin; religious or philosophical belief; trade union membership; political opinion/affiliations</i> ; maiden name; <i>health and disability-related information</i> ; national insurance number (if applicable); tax identification numbers; superannuation selections; spouse & dependant details, next of kin and emergency contact details; signature (including wet ink); and any other information contained in the evidence of identity provided by you on your organisation’s behalf or on your behalf.
Private contact details	Address (including home/office postal address), email address, telephone number (including mobile phone number and home/office number), and emergency contacts, custodian/agent contact information, facsimile number.
Identification data	Photograph; a copy of your driver’s licence and/or passport/identity card and/or other identification documents (including copies of any visas); authorised signatory lists; national insurance number (or equivalent), individual tax number or tax file number (or equivalent), and any other tax-related information; and information we obtain from background verification checks, including information relating to criminal convictions and offences.

<sup>1</sup> ‘Personal Data’ means any information about you from which you can be identified (whether derived from that information on its own or when combined with other information that we or another party may hold about you).



Other categories of data	<p>This may include:</p> <ul style="list-style-type: none"> <li>• Financial related data</li> <li>• Personal information relating to education, employment, medical, etc.</li> <li>• Other information such as directorships and investments</li> <li>• Other information you may choose to disclose.</li> </ul>
Financial related data	Financial information and relationships; credit/financial history; credit/debit card number; expiration date; CVV/CVV2; income/salary; beneficial ownership information; bank account details for individual investors or IFM's vendor/supplier/business partner; and government company registers.
Your education and employment history	CV and cover letter (if applicable); education details; employment history; contractor pay rates; qualifications; technical skills; professional certifications; background checks (including criminal checks); records of reference checks; and records of work absences.
Information relating to your employment with IFM	Start date; role and location of your employment or workplace; details about your remuneration, pension and benefits arrangements (including information on dependants and beneficiaries) and your bank details; flexible working agreements; details of any leave you take or request during our relationship, <i>or sickness absence including health-related information</i> ; details of your travels and expense claims; information about your performance; details of reviews held; details of any bonuses or promotions you receive and other information that relates to your employment; <i>details of any grievance or disciplinary matters, whether brought by or against you or in which you are otherwise involved (which may include sensitive personal information)</i> ; and details of termination or resignation.
Information relating to investments and directorships	Your shareholdings and directorships, including outside directorships, and details of your immediate family members' personal investment holdings and trading activity, which you are required to disclose to us.
Automatically collected Personal Data	CCTV footage (in locations where applicable) including footage or images recorded by video and camera surveillance systems and other information obtained through electronic means such as swipe card or site-access records; information about your use, activity and communications on/from IFM systems and devices, including the dates, times and frequency with which you access the internet, how you use the systems and internet in this way, including the websites you search for and visit and the content you view, and your communications which pass through IFM systems or devices, including emails, instant messages, text messages and app-based messages that you send and receive from your IFM email address. For employees or contractors in particular roles, calls/online meetings/teleconferences may be recorded for a number of reasons (such as quality assurance, training, and compliance requirements).
Information relating to the protection of work products and other assets	<p>Information collected during the course of your employment, including:</p> <ul style="list-style-type: none"> <li>• emails, documents, and other work products and communications created, stored or transmitted using IFM's applications, devices, computers or communications equipment;</li> <li>• log of all emails sent and received on IFM systems, including the name and email address of the sender and recipient(s), the date and time the email was sent, the subject of the email and size of the message;</li> <li>• telephone call logs from IFM office telephones, including numbers called/calling, time and duration of call;</li> <li>• recordings of telephone conversations between third parties and staff using specified telephones, where IFM has legal obligations to make such recordings;</li> <li>• information in relation to internet and email usage by employees of IFM; and</li> <li>• user ID, employee username, system access logs, IP address, browser type, operating system and cookies for certain systems.</li> </ul>
Digital Information	<p>We collect information from you electronically when you use our online services (such as IFM websites). This includes information such as:</p> <ul style="list-style-type: none"> <li>• location information (if enabled on your device);</li> <li>• IP address and range;</li> <li>• information about the electronic devices (computers, mobile phones or tablets) you use to access our platforms and how you use them, including details relating to your devices, their operating systems, browsers, other installed</li> </ul>



	<ul style="list-style-type: none"> <li>applications and settings;</li> <li>details of the wi-fi network or mobile network used by your device; and</li> <li>login data (this is through the client portal), browser type and version, device type, device screen size, time zone setting, browser plug-in types and versions, operating system and platform.</li> </ul>
Other	<p>Extra information (without limitation) that you choose to tell or provide to us (<i>including sensitive Personal Data</i>), or your colleagues, referees, suppliers or professional advisers choose to tell us about you, or that we find from other third-party sources, including social media platforms; Background check details related to the vendor / supplier / business partner (if applicable); Purpose of visit; date of visit, time of visit and any other information which may be provided to facilitate your visit at one of our office locations; Details of an alleged violation/concern and related conduct being reported (including but not limited to date, location, time and relevant circumstances of the concern or conduct).</p> <p>Any Personal Data (<i>including sensitive Personal Data</i>) depending on the nature of the transaction that is provided to us by you or your delegate or that we find from other third-party sources for due diligence exercise.</p>

## How do we collect your Personal Data?

We may collect your Personal Data directly from you. In certain circumstances, we may also collect Personal Data about you from other individuals or third parties. This may include individuals or third parties who handle or process Personal Data on our behalf according to our written instructions.

We may collect Personal Data when you:

- inquire about, apply for, or use our products or services or otherwise engage in business with us
- contact us to make an enquiry, or complaint or give us feedback
- visit our website or one of our IFM offices; and
- apply for a position with IFM or are employed by IFM.

## How do we use your Personal Data?

We may use your Personal Data for the following purposes:

Categories	How do we use your Personal Data
Client and Prospective Client Relationship Management	<ul style="list-style-type: none"> <li>• Manage registration or onboarding and provide requested information.</li> <li>• Offering investment management, advice, and related products and services.</li> <li>• Carrying out due diligence, administrative tasks, and compliance checks (e.g., KYC, anti-money laundering).</li> <li>• Corresponding with you to manage relationships, inform about products/services, or gather feedback.</li> <li>• Ensuring compliance with legal and regulatory obligations (e.g., client identification, counterparty verification).</li> <li>• Administrative, financial accounting, and risk analysis related to service delivery.</li> <li>• Enhance our product and services.</li> </ul>
Investment Execution and Management	<ul style="list-style-type: none"> <li>• Deal management</li> <li>• Supporting in the management of client investment</li> <li>• Payment arrangement</li> <li>• Contract agreements</li> </ul>
Recruitment and Employment Management	<ul style="list-style-type: none"> <li>• Recruitment: Assessing qualifications, contacting you for queries, verifying references, and maintaining recruitment records.</li> <li>• Employment: Managing employment terms, payroll, performance reviews, promotions, and benefits.</li> <li>• Monitoring and managing employee performance, disciplinary actions, and</li> </ul>



	<p>continued suitability for the role.</p> <ul style="list-style-type: none"> <li>Managing compliance with employment and diversity laws, such as health adjustments and equal opportunity reporting.</li> <li>Enhancing our services.</li> </ul>
Security and Safeguarding	<ul style="list-style-type: none"> <li>Ensuring security through the interception of communications, office access controls, and monitoring security incidents.</li> <li>Using CCTV for premises security and ensuring safe travel for employees.</li> <li>Maintaining a safe environment for employees, contractors, and visitors, with security and emergency protocols in place.</li> </ul>
Legal Compliance and Risk Management	<ul style="list-style-type: none"> <li>Complying with applicable laws, including business, financial, and health and safety regulations (e.g., tax collection, crime prevention).</li> <li>Manage conflicts of interest, ensure compliance with regulatory obligations, and conduct legal audits or investigations.</li> <li>Enforcing legal rights, exercising claims, and preventing unlawful activities.</li> </ul>
Vendor and Supplier Relationship Management	<ul style="list-style-type: none"> <li>Making decisions regarding procurement of goods and services, ensuring compliance with policies and regulations.</li> <li>Managing vendor contracts, reporting, and responding to allegations of misconduct or fraud.</li> <li>Communicate news and updates within the IFM and manage business partner relationships.</li> </ul>
Visitor Management and Office Access	<ul style="list-style-type: none"> <li>Facilitating visitor access to IFM offices and ensuring safety and security during visits.</li> <li>Maintaining records for emergency situations, security reviews, and auditing purposes.</li> </ul>
Business Improvement and Feedback	<ul style="list-style-type: none"> <li>Gathering and responding to inquiries, complaints, and feedback on products, services, and customer experiences.</li> <li>Using feedback to improve products, services, and privacy practices.</li> </ul>
Contact Line Management	<ul style="list-style-type: none"> <li>Administering internal business functions, including record maintenance and incident investigations.</li> <li>Compiling statistical data on the use of the Contact Line for reporting and improvement purposes.</li> </ul>

## Why we process your Personal Data?

We process your Personal Data for specified purposes and on the following legal grounds for the various situations which may arise with us:

- When processing your Personal Data, we are relying on the legal basis that processing your Personal Data is within our legitimate interests in pursuing the purposes set out in the table under heading **‘How we use your Personal Data’** (where such interests does not override your interests or fundamental rights or freedoms): namely to:
  - Manage conflicts of interest;
  - Enforce our legal rights or establish, exercise and defend claims; and
  - Run our business in accordance with industry best practices and expectations.
- We may rely on the legal basis that 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.
- When processing your Personal Data, we also rely on the legal basis that the processing is necessary for us to carry out our legal obligations.
- When processing your Personal Data, we may also rely on consent as the legal basis that the processing is necessary for us to carry out our business functions.



## Direct marketing

We may use the Personal Data we collect to send you marketing communications about products, services, or offers that may interest you. You will have the option to opt in or opt out of receiving such communications. If you prefer not to receive direct marketing, you can unsubscribe at any time by following the instructions in the communication or by contacting us directly.

## With whom we share/disclose your Personal Data

We may share/disclose your Personal Data with any of the following parties:

- **IFM:** We may share your Personal Data with IFM members and/or funds managed or advised by IFM and their affiliates to support and manage business operations/activities.
- **Our service providers:** We may share Personal Data with our service providers who assist us in performing our functions and services or perform functions on our behalf. These service providers may include but are not limited to organisations that provide personnel and services such as insurance and insurance broking, archival, recruitment, mail and delivery, private medical and dental, pension scheme administrations, employee training, health and safety, auditing, professional advisory (financial, legal, tax and management consulting), AML/KYC, banking, security or technology services/ support that may also support Generative Artificial Intelligence.
- **Regulators or other authorities:** We may share your information in order to comply with our legal and regulatory obligations, such as regulators, when, in our reasonable opinion, the law or other regulation requires us to share this data. We may also share your Personal Data where we think this is necessary, for example, to meet our legitimate interests and protect our business, including from fraud and legal claims.
- **Other parties as part of a corporate transaction:** We may share your information with prospective purchasers and their advisers when we are discussing selling or transferring part, or all, of an IFM entity to them, so they can evaluate the relevant business. If we are restructured or sold to another organisation, we may transfer information we hold about you to them so they can continue to provide services to you.
- **Funding partners:** We may disclose your Personal Data with other entities, such as finance providers, who we reasonably believe are required to receive the information to enable us to undertake our business activities in the ordinary course of business.

## Data quality

We take reasonable steps to ensure that the information we process is up-to-date and accurate. We encourage individuals to inform us of any changes to their personal details to help us maintain the highest data quality standards. If you believe that any of your Personal Data we hold is incorrect or outdated, please contact us, and we will make the necessary corrections where possible.

## Use of Government Identifiers

We respect your privacy and only collect and use government identifiers (such as social security numbers or national ID numbers or tax file numbers) when absolutely necessary for legal, regulatory, or contractual obligations. IFM does not adopt a government related identifier of an individual as its own identifier of the individual. Any such information will be handled securely and in accordance with applicable laws to protect your rights and confidentiality. We are committed to ensuring that these sensitive data points are stored and processed securely to prevent unauthorised access or misuse.

## Is your Personal Data transferred across international borders?

We may transfer your Personal Data to IFM offices and authorised third parties located outside of your country and take organisational, contractual and legal measures to ensure that your Personal Data are exclusively processed for the purposes mentioned above and that adequate levels of protection have been implemented to safeguard your Personal Data. These transfers will be undertaken in compliance with applicable law(s) and regulation(s).



If it is necessary to transfer your Personal Data from your habitual place of residence to countries that do not offer adequate protections, then we will ensure that appropriate safeguards, as required by applicable laws, are put in place prior to the transfer of the data. For example, incorporating standard contractual clauses or data transfer agreement(s) established between the parties transferring the Personal Data. Further details of these transfers are available upon request.

## **How long do we retain your Personal Data?**

We will take reasonable steps to keep your Personal Data for no longer than is necessary for the purposes for which we collected it, subject to any legal obligation to retain Personal Data for a prescribed period of time as specified in our Records Retention Schedule.

When determining the length of time, we take into account factors such as our legal or regulatory responsibilities, including complying with any required retention periods and limitation periods relevant to legal action. For example, we may need to retain certain of your Personal Data for purposes such as potential litigation or insurance claims.

## **How do we safeguard your Personal Data?**

We implement and maintain appropriate technical, organisational and physical security measures to protect your Personal Data that align with cyber security requirements from certain leading standards (such as the National Institute of Standards and Technology and the International Organisation for Standardisation).

These may include, but are not limited to, the following:

- Access to Personal Data is based on the need-to-know and least privilege principle to ensure that Personal Data is only accessible to authorised individuals for the performance of their duties.
- Layered security controls ranging from perimeter security to end user machine level controls such as firewalls, spam protection, antivirus and spyware solutions, security awareness training, and incident management are applied.
- We use encryption mechanisms, where appropriate, such as email encryption, encryption of Personal Data during transfer, secure VPN access, and disk level encryption, etc.
- Third parties that process Personal Data on our behalf do so according to our written instructions. They are bound by confidentiality and must implement suitable technical and organisational measures to ensure the Personal Data is secured.

If the security of the information is compromised, we take action to mitigate the risk to the individual. We manage and report privacy breaches in a timely manner to regulators as required by law and regulation.

## **Anonymity and pseudonymity**

Wherever possible, IFM evaluates and makes individuals aware of the option of not identifying themselves or of using a pseudonym to protect their privacy. Anonymisation is a tool which may be utilized in our efforts to ensure that Personal Data is handled securely and in accordance with applicable privacy laws.

## **Your rights in relation to your Personal Data**

You have certain rights in relation to the Personal Data IFM holds about you. These rights vary depending on the country where you are based. Further information about your rights, and how you can exercise them, is provided in [Addendum 1](#).

## **Use of Cookies**

IFM and IFM contracted third parties / service providers use cookies and similar tracking technologies to enhance your experience on our website and services. Cookies help us remember your preferences, analyse website traffic, and provide personalised content. You can control cookies in your browser to enable or disable them. If you wish to restrict or block the cookies that are set by any website – including IFM websites – you can do this



through the web browser settings for each web browser you use on each device you use to access the internet. You can opt out of each cookie category except for strictly necessary cookies by making changes to the browser settings. Please note that disabling cookies may affect the functionality of certain parts of our site. [A list of the cookies IFM uses can be found here.](#)

### **Who can you contact if you have a query, concern, or complaint about your Personal Data?**

If you have any issues, queries or complaints regarding the processing of your Personal Data, please contact us at [dataprotection@ifminvestors.com](mailto:dataprotection@ifminvestors.com). For more details, please refer to the section 'Contact Details' above. If you are unsatisfied with the handling of your Personal Data by IFM, please refer to [Addendum 2](#) for the Country/State specific supervisory authority list.

### **How do we update this Statement?**

This external privacy statement was last updated on 11 April 2025.