PRIVACY NOTICE

For Investors, Website Users and Other Third Parties
September 2026

About this privacy notice

This Privacy Notice sets out the basis on which Orbis collects and processes personal data when we deal with our clients and other relevant persons, including:

- investors and prospective investors;
- visitors to our websites;
- service providers, business partners and other business contacts; and
- other individuals who interact with us (together, "you").

References to "Orbis", "we", "us" or "our" are to the relevant Orbis entity that determines the purposes and means of processing your personal data and therefore acts as a data controller.

Orbis regards the lawful and correct treatment of personal data as integral to its operations and necessary to maintain the confidence of its clients, business partners and regulators.

If you are an employee of Orbis or applying for a role with us, please refer instead to the Privacy Notice for Employees and Candidates.

What personal data do we collect?

Orbis collects personal data provided by you, for example during account opening, completing a subscription form, corresponding with us or using the Orbis website. This may include:

- contact information (e.g. name, email address, telephone number);
- personal characteristics (e.g. date of birth, nationality);
- government issued identifiers (e.g. passport details, tax identification numbers);
- transaction information;
- financial information such as bank details and source of wealth; and
- technical information, including IP address and information about website usage.

This list is not exhaustive and Orbis may collect additional personal data where required by law or where it is in our legitimate interests to do so. We limit the personal data we collect to what is necessary for the purposes described in this notice.

If you visit our offices, CCTV may operate in and around our premises for security purposes (see "CCTV" below).

Australia (APP 2)

Where lawful and practicable, individuals may interact with Orbis anonymously — for example, by visiting our website without identifying themselves. However, providing investment services, completing account opening, or making a formal enquiry requires that you identify yourself.

What personal data do we collect from third parties?

We collect personal data from third parties to comply with our legal and regulatory obligations and to operate our business. This includes:

- AML, KYC and sanctions screening providers;
- fraud prevention agencies;
- financial institutions, custodians, distributors and intermediaries;
- publicly available sources; and
- service providers supporting our IT, communications and operations.

Why we use your personal data

We collect and use your personal data to provide our services, to communicate with you and to comply with our legal obligations. The table below sets out each processing purpose and the legal basis on which we rely.

Purpose	Legal basis	Jurisdiction notes
Provide services and service your account	Contract	GDPR / UK-GDPR / Japan APPI / BC PIPA / PIPEDA
Maintain investor records and process transactions	Contract / Legal obligation	All jurisdictions
Comply with AML, KYC and regulatory requirements	Legal obligation	All jurisdictions
Prevent fraud and unauthorised transactions	Legitimate interests — fraud prevention	GDPR / UK-GDPR / Australia APPs
Manage and operate our business	Legitimate interests — business operations	GDPR / UK-GDPR / Australia APPs
Improve products, tools and website	Legitimate interests — service improvement	GDPR / UK-GDPR
Ensure website functionality and security	Legitimate interests — network security	GDPR / UK-GDPR / Australia APPs
Marketing (to existing clients only)	Legitimate interests / Consent where required	GDPR / UK-GDPR / Japan APPI / CASL

A legitimate interests balancing assessment has been conducted for each purpose marked above.

We will only use your personal data for the purposes for which it was collected or for purposes that are directly related to those purposes, unless we obtain your consent or are otherwise permitted by law.

Where personal data is required to comply with legal or contractual obligations, failure to provide such data may result in our inability to provide services or enter a relationship with you.

Legal bases

Where applicable, the legal bases on which we rely are set out in the purpose table above. In summary, we rely on:

- contractual necessity: where processing is necessary to perform a contract with you or to take steps at your request before entering into a contract;
- legal obligations: where processing is required by applicable law or regulation;
- legitimate interests: where processing is necessary for our legitimate interests or those of a third party, provided those interests are not overridden by your interests or fundamental rights. We conduct a balancing assessment for each such purpose; and
- consent: where required, for example for certain marketing communications or non-essential cookies.

Cookies and website usage

We use cookies and similar technologies on our website to improve its performance and enhance your user experience. Cookies help us to:

- recognise your device;
- understand how visitors use our website; and
- improve our services, content and communications.

Where required by law, we will obtain your consent before placing non-essential cookies on your device. For more information, including how to manage or withdraw your consent, please see our Cookie Notice.

Disclosure of your personal data

We may disclose your personal data to:

- other Orbis group entities;
- service providers (IT, legal, audit, communications);
- custodians, administrators and distributors;
- regulators, tax authorities and law enforcement.

Where third parties process personal data on our behalf, they do so in accordance with our instructions and are subject to contractual obligations to implement appropriate technical and organisational measures. We do not sell or share personal data for third-party marketing.

Japan APPI — third-party disclosure

When Orbis discloses personal information to third parties (including Orbis group entities outside Japan), we do so either with your consent, under an applicable APPI exception, or pursuant to a third-party provision agreement notified to the Personal Information Protection Commission (PPC) where an opt-out procedure applies. Intra-group transfers to Orbis entities in other countries are governed by our Binding Corporate Rules and data sharing agreements that require each recipient entity to handle your personal information in accordance with the APPI.

U.S. Regulation S-P

Where U.S. privacy laws apply, including Regulation S-P under the Securities Exchange Act of 1934, Orbis may collect, use and disclose non-public personal information ("NPI") in connection with providing financial services.

We provide an initial notice of our privacy practices when you establish a relationship with us, and an annual notice thereafter, each year that the relationship continues, as required under Regulation S-P.

We do not disclose NPI to non-affiliated third parties except as permitted by law, including for servicing accounts, processing transactions, or through service providers subject to confidentiality obligations.

You have the right to opt out of certain disclosures of NPI to non-affiliated third parties. If you wish to exercise this right, please contact us at privacy@orbis.com.

We maintain physical, electronic and procedural safeguards designed to protect NPI in accordance with Regulation S-P. Where applicable, we maintain a written incident response programme designed to detect, respond to and recover from unauthorised access to or use of customer NPI. In the event of a breach of security involving NPI, we will notify affected individuals as required under Regulation S-P (as amended by the SEC's 2023 amendments), including within 30 days of discovery where the relevant Orbis entity is a registered investment adviser or broker-dealer subject to those requirements.

International transfers

Your personal data may be transferred to and processed in countries outside your country of residence, including within the Orbis group and to our service providers. The table below sets out our key international transfer scenarios and the safeguards we apply.

Destination region	Transfer scenario	Safeguard mechanism
Australia to overseas	Intra-group (South Africa, UK, US, Japan, HK, Bermuda, Canada); fund administrators	APP 8 — contractual obligations requiring overseas recipients to comply with the Australian Privacy Principles; or adequacy assessment
Bermuda to overseas	Intra-group; investment operations	Contractual safeguards consistent with Bermuda PIPA requirements

Destination region	Transfer scenario	Safeguard mechanism
Canada (PIPEDA / BC PIPA) to overseas	Intra-group; payroll / IT providers	Contractual protections ensuring comparable protection; transfers assessed under PIPEDA / BC PIPA
EU to UK / non-EEA	Intra-group transfers; service provider disclosures	EU Standard Contractual Clauses; UK International Data Transfer Agreement (IDTA) for UK-origin transfers
Hong Kong to overseas	Intra-group; service providers	Contractual data protection clauses consistent with PDPO requirements
Japan to overseas	Intra-group; fund administrators	APPI outsourcing agreements; third-party provision agreements with PPC notification where required
UK to non-UK	Intra-group; custodians; technology providers	UK IDTA or UK Addendum to EU SCCs; adequacy regulations where applicable

Australia (APP 5 / APP 8)

If you are an Australian resident, your personal information may be disclosed to recipients in South Africa, the United Kingdom, the United States, Japan, Hong Kong, Bermuda and Canada. Before making any such disclosure, we take reasonable steps to ensure overseas recipients handle your personal information in accordance with the Australian Privacy Principles (APP 8). We remain accountable if an overseas recipient mishandles your information.

How long we hold your personal data

Orbis retains personal data only for so long as is reasonably necessary for the purposes for which it was collected, taking into account legal, regulatory and business requirements. The table below sets out our key retention periods. The retention periods may be longer or shorter as required or permitted by applicable law. Retention periods may vary by document type and jurisdiction.

Data category	Retention period	Legal/regulatory basis	Notes
All client records including account opening forms, transaction records, due diligence, and correspondence.	Orbis SICAV clients: 11 years from the end of the business relationship Orbis OEIC clients: 5 years from the end of the business relationship All other Clients: 11 years from the end of the business relationship	AML Directives (EU/UK); FATF standards; local AML laws	Longer periods may apply where subject to investigation or legal hold
Transaction and account records	5–11 years from end of relationship	Financial services regulation across applicable jurisdictions	Varies by jurisdiction and product type
Investor correspondence	5–11 years from end of relationship	Financial services regulation across applicable jurisdictions	Varies by jurisdiction and product type
Regulatory and compliance records	5–11 years from end of relationship	FCA, SEC, SFC and equivalent regulators	May exceed standard retention

Where appropriate, personal data may be anonymised rather than deleted at the end of the retention period.

Personal data may also appear incidentally within broader business records, for example, in correspondence, working documents, research materials, or the outputs of analytical tools used in our ordinary course of business. Such personal data cannot be isolated from the surrounding record without compromising its integrity or our ability to meet other legal and regulatory obligations, and so this data is retained for as long as the underlying business record is retained under our records retention policies, rather than on a separate schedule. Where we receive a valid request to erase such data, we will assess and act on it in accordance with applicable law, which may include exemptions where isolating or removing the data would require disproportionate effort or would conflict with a legal or regulatory retention obligation.

Security

We maintain appropriate technical and organisational safeguards designed to protect your personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. We apply privacy by design principles in the development of our systems and processes.

Personal data breaches are managed in accordance with Orbis' incident response procedures and, where required by applicable law, reported to the relevant supervisory authority and affected individuals without undue delay. In Canada, we will notify the Office of the Privacy Commissioner of Canada (OPC) and affected individuals of any breach that creates a real risk of significant harm, in accordance with PIPEDA and the Breach of Security Safeguards Regulations. In British Columbia, we will also notify the BC Office of the Information and Privacy Commissioner (OIPC) as required under BC PIPA. We maintain a record of security breaches.

CCTV

CCTV cameras operate in and around our office premises for the purposes of security and safety. CCTV footage is:

- retained for a maximum of 90 days, after which it is automatically overwritten or deleted;
- accessible only to authorised personnel (e.g. security, senior management) on a need-to-know basis; and
- retained for longer only where required in connection with an incident, investigation or legal hold obligation.

If you believe you have been captured on CCTV footage and wish to make a subject access request, please contact privacy@orbis.com. We will respond within 30 days (or the applicable statutory period) and may need to verify your identity before releasing footage.

Use of technology and automated processing

We may use data analytics and artificial intelligence–based tools to support our operations, compliance monitoring and decision-making.

We do not make decisions that produce legal or similarly significant effects on individuals based solely on automated processing without human review. Where automated tools are used to assist in decision-making (for example, in transaction monitoring or fraud detection), a human reviewer considers the output before any decision is made.

Australia (APP update — automated decision-making disclosure, effective December 2026)

From December 2026, Australian entities will be required to disclose when personal information is used to make, or assist in making, a decision that significantly affects an individual. We will update this notice to include the required disclosure before that date.

Direct marketing

Where we have your consent or a legitimate interest to do so, we may contact you with information about our products and services.

You may opt out of direct marketing at any time by:

- clicking the unsubscribe link in any marketing communication;
- emailing privacy@orbis.com with the subject line "Marketing opt-out"; or
- for Canadian residents, withdrawing consent in accordance with Canada's Anti-Spam Legislation (CASL) by emailing privacy@orbis.com.



We will process your opt-out request within 10 business days. Opting out of marketing does not affect any other processing of your personal data.

Your legal rights

Depending on your jurisdiction, you may have the following rights in relation to your personal data:

- right of access — to obtain a copy of your personal data and information about how it is processed;
- right to rectification — to have inaccurate personal data corrected;
- right to erasure — in certain circumstances, to have your personal data deleted;
- right to restrict processing — to limit how we use your personal data;
- right to data portability — in certain circumstances, to receive your data in a structured, machine-readable format;
- right to object — to processing based on legitimate interests, including direct marketing; and
- right to withdraw consent — at any time, without affecting the lawfulness of prior processing.

To exercise any of these rights, please contact privacy@orbis.com. We will respond within 30 days (or the applicable statutory period). We may ask you to verify your identity before processing your request.

Australia (Australian Privacy Principles)

If you are an Australian resident, you have rights under the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs), including:

- APP 12: the right to request access to personal information we hold about you. We will respond within 30 days. We will not charge you for making a request but may charge a reasonable fee for providing access.
- APP 13: the right to request correction of personal information that is inaccurate, out of date, incomplete or misleading. If we decline to correct information, you may request that we associate a statement of disagreement with the record.
- APP 7: the right to opt out of direct marketing at any time.

To lodge a privacy complaint, please contact privacy@orbis.com. If your complaint is not resolved within 30 days, you may refer it to the Office of the Australian Information Commissioner (OAIC): www.oaic.gov.au.

Bermuda (PIPA)

Orbis Investment Management Limited is the responsible organisation for personal data processed in Bermuda. You have the right to access and correct your personal data under sections 14–15 of the Bermuda Personal Information Protection Act. Requests should be directed to privacy@orbis.com. Unresolved complaints may be referred to the Privacy Commissioner for Bermuda.

California (CCPA / CPRA)

If you are a California resident, you may have the following rights under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA):

- Right to know: to request information about the categories and specific pieces of personal information we collect, the purposes for which we use it, and the categories of third parties to whom we disclose it.

- Right to delete: to request deletion of personal information we hold about you, subject to certain exceptions.
- Right to correct: to request correction of inaccurate personal information.
- Right to opt out of sale or sharing: Orbis does not sell personal information or share it for cross-context behavioural advertising. If this practice changes, we will update this notice and provide a "Do Not Sell or Share My Personal Information" mechanism.
- Right to limit use of sensitive personal information: to request that we limit our use of sensitive personal information to the purposes permitted under CPRA.
- Right to non-discrimination: we will not discriminate against you for exercising any of your CCPA/CPRA rights.

To submit a request, or to designate an authorised agent to submit a request on your behalf, please contact us at privacy@orbis.com. We will respond within 45 days (extendable by a further 45 days where reasonably necessary).

Canada (PIPEDA and BC PIPA)

Our Privacy Officer is responsible for compliance with PIPEDA and BC PIPA. Contact: privacy@orbis.com. You may submit an access request or complaint to the Privacy Officer. If your complaint is not resolved to your satisfaction, you may escalate to:

- Office of the Privacy Commissioner of Canada (OPC): www.priv.gc.ca
- BC Office of the Information and Privacy Commissioner (OIPC): www.oipc.bc.ca

EU — Supervisory Authority

If you are based in the EU and wish to lodge a complaint about our handling of your personal data, you may contact the data protection authority in your country of residence or the country where the alleged infringement took place. Details of EU data protection authorities are available at: www.edpb.europa.eu/about-edpb/about-edpb/members_en

Hong Kong — Personal Data (Privacy) Ordinance (PDPO)

Under the PDPO, you have the right to request access to and correction of your personal data. Requests should be directed in writing to the Data Access Request Officer, privacy@orbis.com. We will acknowledge your request within 10 days and respond within 40 days (or seek an extension as permitted by law).

If you are based in Hong Kong and your complaint is not resolved to your satisfaction, you may refer it to the Office of the Privacy Commissioner for Personal Data (PCPD): www.pcpd.org.hk.

Japan — Personal Information Protection Commission (PPC)

You have the right under APPI Arts. 33–39 to request disclosure, correction, addition, deletion or cessation of use of your personal information. If you are based in Japan and wish to escalate a complaint, you may contact the Personal Information Protection Commission (PPC): www.ppc.go.jp.

UK — Information Commissioner's Office (ICO)

If you are based in the UK and wish to lodge a complaint about our handling of your personal data under the UK GDPR or the Data Protection Act 2018, you may contact the Information Commissioner's Office (ICO): www.ico.org.uk. The ICO can be reached by telephone on 0303 123 1113.

Changes to this notice

We may update this Privacy Notice from time to time to reflect changes in applicable law, our data practices or our business. Any material changes will be posted on our website. Where required by applicable law, we will notify you directly.

Contact

If you have any questions about this notice or how we handle your personal data, please contact our Privacy Officer. Email: privacy@orbis.com