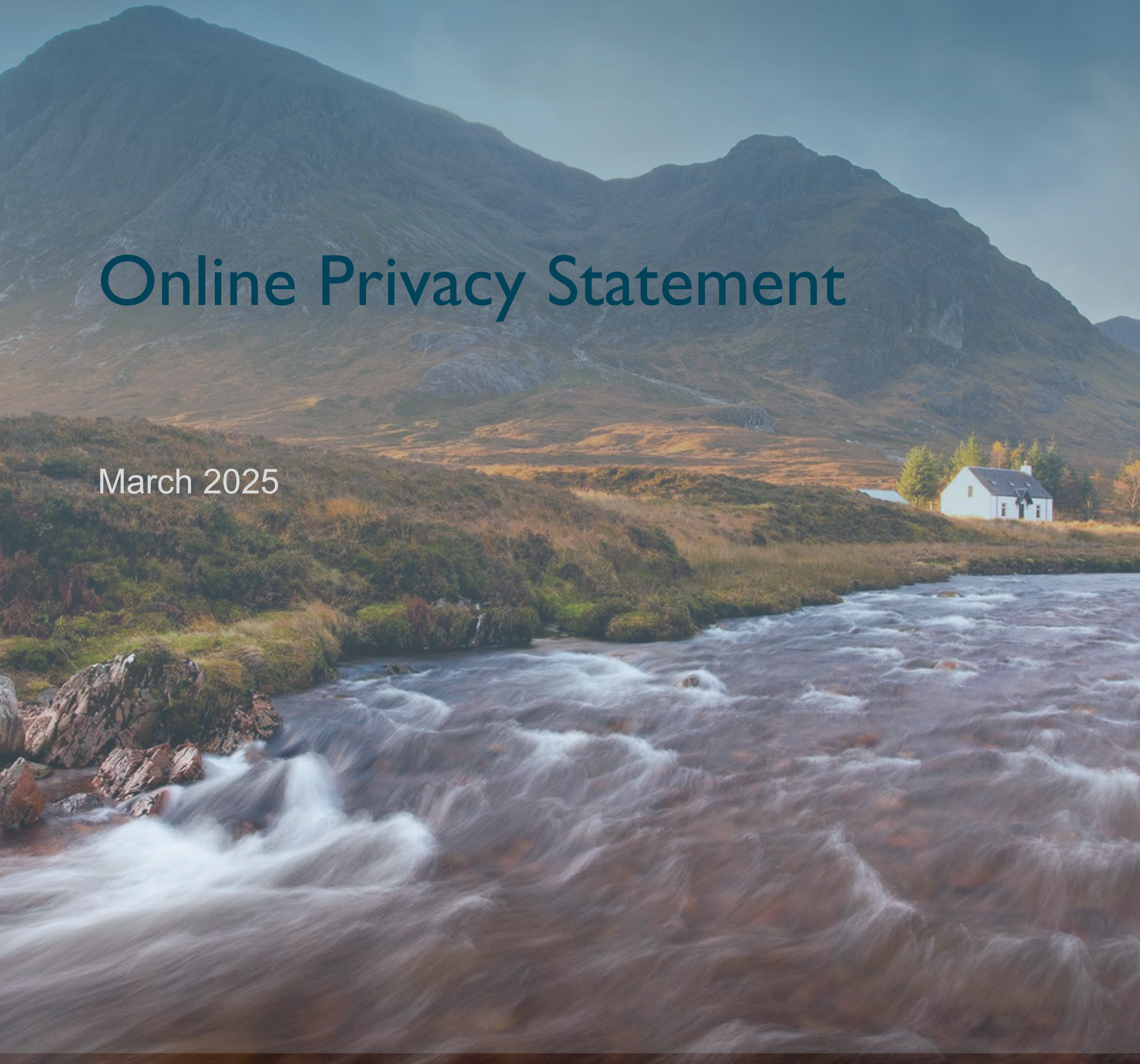
Hosking Partners®

Online Privacy Statement

March 2025



ONLINE PRIVACY STATEMENT

This Privacy Notice explains how we collect, use, disclose, store, and share your personal information. It applies to personal information provided to us, both by you and by others on your behalf. It also explains the rights you may have in relation to the personal information that we hold about you.

We have developed this Privacy Notice because Hosking Partners LLP (“HPL”) is committed to complying with the applicable data privacy and security requirements in the countries in which it operates, including, but not limited to, the UK Data Protection Act and the UK General Data Protection Regulation (UK GDPR).

When we refer to “personal information” or “personal data" in this Privacy Notice, we mean information which identifies you as an individual, or is capable of doing so. In the context of this Privacy Notice, the terms “personal information” and “personal data” may be used interchangeably.

This Privacy Notice applies to HPL while running its business and providing asset management services (the "services") to its customers. This statement describes:

Please click on the relevant heading above for more information on each of these areas.

1. WHAT PERSONAL INFORMATION DO WE COLLECT ABOUT YOU?

The personal information which we may collect will generally consist of:

- information about you – for example name, age, gender, title, date of birth and nationality. We need this information to help us identify you, but also to allow us to contact you, for example, for regulatory or service reporting reasons; and
- contact information - for example email, address, postcode, and phone number.

In certain circumstances we may also need to collect and use:

- government identifiers – for example identification document information (driving licence, passport) and National Insurance number;
- financial information – bank account details for any payments you make to us, or we make to you; and
- audio or video recordings – for example voice recording when you contact us, or CCTV footage if you visit our offices. Calls may be recorded for regulatory purposes, such as calls relating to the reception, transmission, and execution of investment orders;

If we do not collect, or you do not provide, your personal information to us, we may not be able to provide our services to you or engage your services (as applicable).

If you apply for a job with us, we will hold and process personal information relevant to recruitment which may include CVs, references, and DBS checks.

2. HOW DO WE OBTAIN YOUR PERSONAL INFORMATION?

Most of the information we receive comes directly from you as a client, contact, supplier, from your financial adviser or intermediary if you have appointed one, or from public record. This will include provision of business cards when you meet an HPL representative, at the point these are subsequently added to our internal database.

We may also get personal information about you from other sources, such as:

- Web search – we may search for contact details over the web. In this case, we will tell you at first contact where we got your details from;
- Events list – we also get names through lists of events that we sponsor. In this case, we ask the organiser to only share the contacts that agreed to be contacted;
- Business intelligence portals – sometimes we get contact details of employees of institutions we would like to work with from portals that we subscribe to. These portals provide information on industry trends where personal data could be provided;
- Your employer – when an institution becomes our client, they may have provided your details as the person we contact; and
- Risk & compliance portals – we use information from third-party portals to conduct regulatory checks.

If you apply for a job with us, we may collect information either directly from you or from third parties including employment agencies, former employers, other referees, background check agencies or publicly available information.

3. USE OF ANALYTICS AND COOKIES

Hosking Partners only employs essential cookies in respect of its website, to ensure the platform is safe, secure, and working efficiently for users. A complete list of cookies used on the website, their purpose, and the duration the related information is retained is listed below.

Cookie name	Purpose	Duration	Cookie Type
XSFR-TOKEN	Used for security reasons	Session	Essential
hs	Used for security reasons	Session	Essential
svSession	Used in connection with user login	12 months	Essential
SSR-caching	Used to indicate the system from which the site was rendered	1 minute	Essential
_wixCIDX	Used for system monitoring/debugging	3 months	Essential
_wix_browser_sess	Used for system monitoring/debugging	Session	Essential
smSession	Used to identify logged in site members	Session	Essential
TS*	Used for security and anti-fraud reasons	Session	Essential
bSession	Used for system effectiveness measurement	30 minutes	Essential
Fedops.logger.X	Used for stability/effectiveness measurement	12 months	Essential

4. HOW DO WE USE YOUR PERSONAL INFORMATION?

We use any information we obtain for a number of reasons. Depending on which category you fit into, we have different processing activities which may be conducted by us directly or trusted third party companies that we use. We use information in the following ways for each category:

a) If you are an investor in one of our funds or an employee or officer of such an investor:

- fulfilling any legal, compliance, regulatory and reporting obligations;
- facilitating the management and administration of your investment including fee invoicing, completing any request you make and updating you to proposed changes to the pooled fund in which you may be invested or in relation to HPL generally;

- maintaining a backup investment register for business continuity purposes; and
- providing marketing information or presentations on HPL and its products or informing you of our investment views and market commentaries from time to time;

b) If you are client investing through a segregated mandate or an employee or officer, of such client:

- processing your investment application;
- verifying your identity and preventing fraud;
- fulfilling any legal, compliance, regulatory and reporting obligations;
- facilitating the management and administration of your investment including fee invoicing, completing any request you make and updating you to proposed changes to the pooled fund in which you may be invested or in relation to HPL generally; and
- providing marketing information or presentations on HPL and its products or informing you of our investment views and market commentaries from time to time;

c) If you are an adviser, investment consultant, wealth manager, an employee of a potential institutional client or pooled fund investor, or are exercising investment control for an institutional client:

- verifying your identity and preventing fraud;
- fulfilling any legal, compliance, regulatory and reporting obligations;
- managing the relationship with our institutional clients and pooled fund investors;
- assessing and developing our products, systems, prices, and brand; and
- providing marketing information or presentations on HPL and its products or informing you of our investment views and market commentaries from time to time.

d) If you are the contact of one of our existing or potential suppliers, agents, consultants, service providers or advisers:

- To run our business affairs and to enable provision of our client services.

e) If you apply for a job with us, we may process recruitment information to ensure that we are recruiting employees with the appropriate skills, qualification, experience, and suitability for each role.

Processing activities that apply to all the people whose personal information we process:

- recording phone calls if you call one of our recorded lines;
- recording MS Teams / Zoom meetings for internal usage; and
- recording CCTV footage if you visit our offices.

5. WHAT ARE OUR GROUNDS FOR USING YOUR PERSONAL INFORMATION?

Grounds	Uses of your information
Necessary for compliance with a legal obligation The personal information you provide may be processed when we have a legal obligation to perform such processing. For example, where we share information with our regulators, auditors, or the courts.	**Verifying your identity and preventing fraud (investors, controlling persons)** We may verify your identity and perform Know Your Client (KYC) checks to comply with regulatory obligations to which HPL is subject. We sometimes need copies of your identification documents such as passport or driving licence. This is to ensure we meet our obligations with anti-money laundering or other such laws. **Fulfilling legal, compliance, regulatory and reporting requirements** HPL is an Alternative Investment Fund Manager (AIFM) and is required by law to adhere to the regulatory requirements accordingly. We need to comply with local (HM Revenue and Customs) and international tax regulation. HPL is regulated by the Financial Conduct Authority (FCA) in the UK as well as with our other international regulators. We are required to make periodic reports to these regulators and provide information on request. **Record phone / video calls** We have a legal requirement under applicable regulations to record the phone lines of our employees that work in reception, transmission, and execution of investment orders. Video calls through MS Teams, Zoom or other similar platforms may also be recorded if related to the transmission and execution of investment orders.

Necessary for legitimate interests of the Firm We may also use your information when we have a "legitimate interest," and that interest is not overridden by your individual rights and freedoms. If you would like further information about processing under legitimate interest, you can contact us using the details below. You have the right to object to any processing done in respect of your personal data for the purpose of our legitimate interests. We will re-assess the balance between our interests and yours, considering your particular circumstances. If we have a compelling reason, we may continue to use your data. For personal information used for marketing purposes, you have the same right to object as set out above, but any objection will result in the cessation of processing immediately on receipt. We use legitimate interests for the following:

Use of your information	Legitimate interest(s)
Facilitating the management and administration of investments in the accordance with contract terms We may hold your personal data as an appointed contact of an institutional client, as an appointed contact of an institution invested in one of our pooled vehicles or in some circumstances as an individual invested in one of our pooled vehicles. We believe it is in the legitimate interests of the business and our investors to use your personal data to fulfil our contractual obligations as set out in our investment management agreements or in accordance with our management agreement with our pooled vehicles. **Managing relationships with our institutional clients** If you were appointed as a contact by an institutional client of ours, this covers: - contacting you for the effective performance of our contract or the contract between yourself and one of our Funds - managing any queries or requests you make	In the legitimate interests of the efficient running of the business, your information may be used to: - facilitate opening a client account with HPL or one of the collective investment vehicles managed by HPL - facilitate processing of subscriptions or redemptions, fee invoicing and other administrative functions including verification of your instructions - completing any ad hoc requests, you make - keeping you updated about your investment and HPL, such as sending you regular statements and performance reports We need to communicate with you to ensure efficient running of the business and that you remain updated in respect of the services provided to you or your customer(s). **Record video calls** On occasion, in addition to those calls required to be recorded for legal purposes, we may record calls to assist with the writing of minutes. You can always request that a call is not recorded. Calls are not shared with third parties without the specific consent of all attendees.

Evolving our products and brand including direct marketing To develop and tailor our services and investment vehicles, we may use information to identify customer groups that are likely to benefit from specific HPL services or investment vehicles. We may also obtain feedback and conduct research in a number of different ways including new fund launches. We will always take steps to check that you have not objected to such contact.	We need to be able to identify gaps in the market and groups of customers who might be interested in new products and services we are considering. We need to make sure our communications and reporting are easy to understand and that they are distributed to the correct audience.
Sending you electronic communications with thought pieces and industry commentary or calling you to enquire if you would like information about products and services If you are an investment consultant, wealth manager or work for our existing or potential clients, we could contact you to send you information on your investment or on investment products that you may be interested in. We may also send commentary on the current markets that may be of use or of interest to you. We will not do this if you have advised us, you do not wish to receive this information. We may send you invitations to meetings or other general events. We will not do this if you have advised us, you do not wish to receive this information. We may source contact information in order to market new products to you or promote brand awareness and the benefits of your existing products. We may analyse your personal information to create a profile so that we can contact you only with information most relevant to you. Where any marketing electronic communications are sent to private individuals, freely given, specific, affirmative consent will be obtained before any correspondence is sent.	We need to grow and sustain our business and develop our brand and effectively communicate with institutions and wealth managers. We believe it is also in your legitimate interest to have all information you need and to be kept up to date with the latest developments in the industry and in our business. Any marketing is highly focussed and has minimal privacy impact. We do not market to retail individuals. You have a right at any time to stop us from contacting you for marketing purposes. If you no longer wish to be contacted for marketing purposes, please email us at dataofficer@hoskingpartners.com or write to us using the information at the end of this notice.

Maintain backup of our investment register For business continuity purposes, we maintain a backup of the holdings and flows of our funds.	We believe it is in our and the investor's legitimate interests that we have a plan in place to ensure smooth recovery in the case of incidents happening to other processors for our collective investment vehicles.
Communication with suppliers, service providers, current or prospective employees, brokers, and advisers For the purpose of running our business in an efficient and effective manner.	We believe it is in our legitimate interests and those of our clients to communicate efficiently with our suppliers, current or prospective employees, brokers, and advisers to ensure the smooth running and efficient operation of the business.
Consent For the purpose of running our business in an efficient and effective manner.	In rare circumstances, we may be asked to send thought pieces or industry commentary or other marketing material to a private in email address. In those particular circumstances, we will ensure that affirmative, specific, freely given consent is obtained to hold and process your data. You can contact us at any time to withdraw this consent by using the contact information at the bottom of this email.
Recruitment For the purpose of running our business in an efficient and effective manner.	The legal basis for processing your personal information relating to recruitment is because it is necessary for our legitimate interests in operating our business efficiently. Where we process your information for DBS checks, this is because it is necessary in connection with employment law or regulatory rights, obligations, and requirements.

6. HOW LONG DO WE KEEP YOUR PERSONAL INFORMATION?

We will keep your personal information for as long as it is considered necessary, for the purpose for which it was collected, and to comply with our legal and regulatory requirements. This will involve keeping your information for a reasonable period of time after your investment or your relationship with us has ended.

Upon expiry of the applicable retention period, we will, to the extent reasonably feasible, securely destroy your Personal Data in accordance with applicable laws and regulations.

7. WHO DO WE SHARE YOUR PERSONAL INFORMATION WITH?

As you would expect, our employees will access your records in order to use your information for the uses mentioned above. However, only those employees who need access to particular information are given it. We regularly check who has access to our systems.

If you are an investor, or consultant to an investor in our Irish Funds, your data is shared with the Fund, which uses it as a data controller in their own right. All rights afforded to you as a data subject under GDPR for data controlled by the Fund are covered by the Fund's data privacy statement and shall be solely exercisable against the Fund.

If you are an investor, or consultant to an investor in an investment vehicle based outside the EU, the data the Fund or Trust control in relation to you is subject to the Data Privacy laws applicable in that jurisdiction.

We may also share your personal information with these categories of third parties:

- Our service providers, Collective Investment Vehicle counterparties and agents e.g. Fund Administrators, Fund Management Companies, depository, trustees and transfer agents, confidential waste disposal and IT companies who support our technology;
- Our professional advisers: auditors, regulatory and legal advisers;
- Identity authentication and fraud prevention agencies;
- HM Revenue & Customs, regulators such as the FCA and SEC and other authorities such as the Information Commissioner's Office;
- Your financial adviser(s) / agent where you have given your authority;
- Organisations that introduce you to us;
- Companies you ask us to share your information with.

We do not sell, rent, or otherwise make personal information commercially available to any third party.

8. HOW DO WE PROTECT YOUR PERSONAL INFORMATION?

We use a variety of technical and organisational measures to help protect your personal information from unauthorised access, use, disclosure, alteration, or destruction consistent with applicable data protection laws.

Although all emails are scanned by cybersecurity software and an anti-virus security centre end point, we recommend you do not send anything confidential to us by email unless password protection has been utilised.

In line with other operational risks, Hosking Partners has established risk management systems and controls as part of its business continuity arrangements that are designed to reduce the risks associated with cyber security including encryption of data, use of passwords, restrictions on remote access, firewall and malware protection as well as ensuring that employees are aware of cyber security risks. All third-party processors commit to a required level of data security included in their contracts. Material outsourced services are subject to due diligence visits to review the controls in place.

In addition, the firm's outsourced IT provider, which hosts our servers and email communication system, is compliant with ISO 27001 Information Security Management System (ISMS) – an internationally recognized best practice management standard for information security. The ISO standard is a framework for effectively assessing and managing risk to the organization.

To achieve this, the standard details a series of core clauses, along with an annex of controls intended to address every area of information security. All these clauses and controls are in the IT provider's ISMS scope. The ISMS is audited annually to ensure compliance with the standard.

Our IT provider is also certified as compliant with the UK Government's Cyber Essentials Scheme which addresses; (i) different types and levels of cyber threats; (ii) vulnerabilities, weaknesses, and exploits; and (iii) their impact.

9. WHICH COUNTRIES DO WE TRANSFER YOUR PERSONAL INFORMATION TO?

To provide our services, we may need to transfer your personal information to locations outside the jurisdiction in which you provide it for the purposes set out in this Privacy Statement. We may sometimes use third parties located in other countries to provide support services. Your data may also be transferred in or out of the EEA to agents, investment consultant and advisers or other companies at your request.

We may also have individual HPL partners or employees working from outside the EEA over a prolonged period of time. HPL partners and employees will utilise the same IT systems as those based within the United Kingdom and are subject to the same training and HPL's internal Data Protection Policy.

Third party services will be conducted by experienced and reputable organisations on terms which safeguard the security of your information and comply with UK and European data protection requirements. Some countries, including those within the EEA, have been assessed by the UK as being 'adequate,' which means their legal system offers a level of protection for personal information which is equal to the UK's protection. Where the country has not been assessed as adequate, we will ensure appropriate standards and processes through the addition of standard contractual clauses.

Since leaving the EU, the UK has recognised its own 'standard contractual clauses' as offering adequate safeguards to protect your rights and we will use these where required, ensuring adequate protection for your information.

We always ensure all personal information is provided with adequate protection and all transfers of personal information outside the EEA are done lawfully.

10. YOUR RIGHTS REGARDING YOUR PERSONAL INFORMATION

The UK's General Data Protection Regulation and other applicable data protection laws provide certain rights for data subjects.

Your rights are outlined below. The easiest way to exercise any of your rights would be to contact our Compliance Department at the contact details provided. We will provide a response within 30 days, if not sooner. There is normally no charge for exercising any of your rights.

You are entitled to request a copy of the information we hold about you and information about how we process it. You may also have a right in accordance with applicable data protection law to have it rectified or deleted, to restrict or suspend our processing of that information, to object to our processing of your information and, in some circumstances, to request receipt or transmission to another organisation, in a machine-readable form, personal information relating to you that you have provided to us.

Where we rely on your consent to process your personal information, you have the right to withdraw your consent at any time.

If you object to the processing of your personal information, or if you have provided your consent to processing and you later choose to withdraw it, we will respect that choice in accordance with our legal obligations. Your objection (or withdrawal of any previously given consent) could mean that we are unable to perform the actions necessary to achieve the purposes set out above (see section entitled 'How do we use your personal information') or that you may not be able to make use of the services and products offered by us. You also have the right to object to any processing done under legitimate interest. We will re-assess the balance between our interests and yours, considering your particular circumstances. If we have a compelling reason, we may continue to use your information. You have a specific right to object to our use of your information for direct marketing purposes, upon which we will always act.

Please note that even after you have chosen to withdraw your consent, we may be able to continue to process your personal information to the extent required or otherwise permitted by law, in connection with exercising and defending our legal rights or meeting our legal and regulatory obligations.

We must ensure that your personal information is accurate and up to date. Therefore, please advise us of any changes to your information by emailing: dataofficer@hoskingpartners.com. If you have any reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of any personal information you might have sent to us has been compromised), please immediately notify us (see section below 'Who to contact with questions or concerns').

11. WHO ARE THE DATA CONTROLLERS?

Hosking Partners LLP is the principal data controller.

12. CHANGES TO OUR PRIVACY STATEMENT

If we want to use your personal information for a new purpose which we have not previously told you about, we will contact you to explain the new use of your information. We will set out why we are using it and our legal reasons.

Any changes we make to this Privacy Statement in the future will be posted on this page and, where appropriate, notified to you by e-mail. The updated Privacy Statement will take effect as soon as it has been updated or otherwise communicated to you. This Privacy Statement was last updated in January 2025.

13. WHO TO CONTACT WITH QUESTIONS, CONCERNS OR COMPLAINTS

If you have complaints, questions or concerns about Data Protection, please contact dataofficer@hoskingpartners.com or write to the Compliance Department at Hosking Partners LLP, 11 Charles II Street, London, SW1Y 4QU or call 0044 207 004 7850.

If you are unhappy with how we are using your information, you have the right to complain to the Information Commissioner's Office. However, we would encourage you to contact us first, so we can have the opportunity to deal with your concerns.

The United Kingdom's Information Commissioner's Office can be contacted at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.