

I-ENVIRONMENT INVESTMENTS LIMITED

WEBSITE PRIVACY STATEMENT

I-Environment Investments Limited (**IEI, we, our, or us**) respects individuals' privacy rights and takes its responsibilities under the data protection and privacy laws seriously.

This Privacy Statement explains how and why we use personal data and what we do to ensure that your information is kept safe and secure in accordance with the Data Protection Act 2018, the UK GDPR and any other applicable data protection and privacy laws (**Data Protection Laws**).

This privacy statement explains:

1. Who we are and how to contact us
2. How we collect and process personal data:
 - A. Information relating to transactions and investments
 - B. Business, professional and other contacts
 - C. Recruitment
3. Website Visitors
4. Recipients of personal data
5. How long we store personal data for
6. How we keep personal data safe
7. International transfers
8. Your rights as a data subject
9. Updates to this statement

1. WHO WE ARE AND HOW TO CONTACT US

IEI is a private limited company with registered number 07585988, having its registered office and main place of business at The Broadgate Tower, 20 Primrose Street, London, EC2A 2EW. You can contact us by writing to us at our office address or emailing enquiries@ieiltd.co.uk with the subject heading "Data Protection".

IEI is part of the ITOCHU Group of companies, which is ultimately owned by ITOCHU Corporation, a company headquartered in Japan and which is listed on the Tokyo Stock Exchange.

For the purposes of Data Protection Laws, IEI is a controller in relation to much of the personal data we collect and process. This means we are responsible for deciding how and why we use personal data and for keeping it safe. IEI is registered as a controller with the Information Commissioner's Office (ICO) with registration number ZB904184.

2. HOW WE COLLECT AND PROCESS PERSONAL DATA

A. INFORMATION RELATING TO TRANSACTIONS AND INVESTMENTS

IEI's business involves making, holding and managing investments in a range of water and waste projects in the UK and EMEA regions. As part of the process of investing, IEI will carry out a due diligence on a project or business including the directors, employees and other individuals involved. This will result in IEI processing information about the directors, employees, contractors as well as suppliers and customers. The information we process may include some or all of the following:

- Details of directors and key employees, including professional experience and qualifications. Occasionally, we may carry out background checks on certain individuals.
- Employee information, including name, date of birth and employment information (such as start date, salary, pension information and social security or national insurance information).

- Information about disciplinary actions, grievances, complaints and similar matters involving current and previous employees.
- Business and professional contact information (of the type described in the section 2.B of this policy) relating to companies we invest in and their shareholders.

In some cases, we may also process sensitive information (also known as 'special category data'), for example information about employees who are absent from work due to illness, or accidents at work.

This information is typically provided to us by the companies we invest in, their shareholders and their advisors. We process this information because we have a legitimate interest (under Article 6(1)(f) UK GDPR) in doing when reviewing the proposed investments and assessing the risks and opportunities involved. This information may be shared with the ITOCHU Group and our professional advisors.

B. BUSINESS, PROFESSIONAL AND OTHER CONTACTS

We collect and process personal data relating to business contacts and other individuals we deal with. Usually this information is either:

- provided by the individuals themselves;
- collected in the ordinary course of business (for example, email correspondence);
- provided to us by third parties (such as other businesses we work with); or
- obtained from external sources (such as company websites or public registers).

The types of personal data we hold about these individuals is typically limited to contact information (such as name, address, telephone and email address). If the individual is a supplier of IEL, then we may also process bank or payment information. There may be situations where we may process other types of personal data. If we do, then it will be protected to the same high standard.

We typically use information about business contacts to pursue our legitimate interest (under Article 6(1)(f) UK GDPR) in building and maintaining business contacts and relationships, as well as carrying on business in the ordinary course. This includes dealing with suppliers, service providers and professional advisers. In some cases, depending on the nature of the information, we may also be required to process the information in order to comply with a legal obligation (for example, relating to tax or accounting records) under Article 6(1)(c) UK GDPR.

C. RECRUITMENT

We collect, store and use personal data about individuals who apply to join us. This may include information:

- you provide to us (such as in CVs, application forms, and in correspondence);
- you provide during an interview;
- obtained from previous employers and referees;
- provided to us by recruitment agencies; and
- received as a result of our carrying out background checks.

The information we collect may include sensitive personal data, such as information about your health and sickness records as well as disability information. If we need to process sensitive personal data then we will ask for your explicit consent before doing so.

If you apply for a job with us, we may carry out a check for criminal convictions in order to satisfy ourselves that there is nothing in your history which makes you unsuitable for the role. We do this because working with us involves a high degree of trust (as you will have access to confidential information). We only carry out criminal records checks and ask for references at the last stage of the application process, when making an offer of employment, and always act in accordance with the specific requirements of Data Protection Laws and other applicable national laws.

How we use applicant information and our lawful basis

We use the personal data we collect about you to:

- assess your skills, qualifications, and suitability for a role;
- carry out background and reference checks;
- communicate with you about your application;
- keep records related to our hiring process.

We do all of this because either it is a necessary part of entering into a contract of employment with you (Article 6(1)(a) UK GDPR) or because we have a legitimate interest in ensuring that you are suitable for employment (Article 6(1)(f) UK GDPR). If you fail to provide personal data when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully.

If we need to process sensitive personal data about a job applicant, for example disability information (to consider whether we need to provide appropriate adjustments during the recruitment process), we will ask for explicit consent to do or ensure that we satisfy another condition under Data Protection Laws for lawfully processing such personal data.

We normally retain personal data about unsuccessful candidates for no more than 6 months from the time we inform them of our hiring decision. We retain personal data for this period so that we can demonstrate, in the event of a legal claim, we have not discriminated against an applicant and that the recruitment process was fair and transparent. After this period, we will securely destroy the applicant's personal data. If we wish to retain personal data on file, in case future opportunities arise, we will contact the applicant and ask for his or her consent to do so. If you are successful, the personal data you provided in the application process will be stored as part of your personnel file.

3. COOKIES AND WEBSITE VISITORS

We do not normally collect personal data about visitors to our website unless they choose to provide such information when contacting us.

Hyperlinks to other sites

Our website may include links to third-party websites or to other software applications or plug-ins. We are not responsible for the content or functionality of any of those external websites. If an external website requests personal information from you, the information you provide will not be covered by this statement. We suggest you read the privacy policy of any website before providing any personal information.

4. RECIPIENTS OF PERSONAL DATA

Personal data you provide to us will be kept private and confidential, and we will only disclose or share it with other data controllers where this is required:

- in connection with our business and investments. For example, we may share information with professional advisors and parties to an investment transaction that we are involved in;
- by law, such as where we are required to comply with a court order or to share personal information with regulatory authorities in the event of an audit or investigation;
- where we have satisfied ourselves that we have another lawful basis for sharing your personal data; or
- in connection with a business reorganisation, merger, acquisition or other corporate transaction affecting IEI, in order to allow the parties to evaluate the transaction and to ensure that our clients continue to receive our goods and services without interruption.

We share your personal data with ITOCHU Europe PLC and other companies in the ITOCHU Group, which provide services to IEI. We may also share personal data with the third parties who provide services to IEI. This includes software, cloud and IT service providers. However, these third parties will only process personal data (which may include your information) on our behalf for specified purposes and in accordance with our strict instructions.

We only use third party service providers who have provided sufficient guarantees, as required by Data Protection Laws, that your personal data will be kept safe. We always ensure there is a written contract in place which protects your personal data and prevents it from being used for any purpose other than providing services to our business, in accordance with Data Protection Laws.

5. HOW LONG WE STORE PERSONAL DATA FOR

We only retain personal data for as long as is necessary for the specific purpose(s) it was collected for (or for related compatible purposes such as complying with applicable legal, accounting, or record-keeping requirements).

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from its unauthorised use or disclosure, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

6. HOW WE KEEP PERSONAL DATA SAFE

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, damaged or destroyed, altered or disclosed. This includes both physical security measures (such as keeping paper files in secure, access-controlled premises which are monitored by CCTV), adhering to strict password policies and IT security (such as device encryption, digital back-ups and sophisticated anti-virus protection).

We limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to legal and contractual confidentiality obligations.

We have put in place reporting procedures to deal with any suspected personal data breach and will notify you and any applicable supervisory authority of a breach when we are legally required to do so.

7. INTERNATIONAL TRANSFERS

We normally only store personal data within the UK. However, there are some circumstances when information may be transferred outside the UK. These include when IEI:

- Uses technology and support services we use are provided by service providers based in other countries;
- shares information within the ITOCHU Group, which will involve transferring it to Japan and other countries outside the UK; or
- is involved in projects or is transactions outside the UK, such as our investments in the EMEA region. In these situations, limited amounts of information relating to that project or transaction may be transferred outside the UK. For example, to advisors in the relevant jurisdiction.

Before transferring personal data outside the UK, we take steps to make sure that any personal data they process is adequately protected and transferred in accordance with Data Protection Laws, usually by one or more of the following methods:

- ensuring the recipient is in a country which has been approved in accordance with Data Protection Laws as providing adequate protection for personal data;
- implementing appropriate safeguards such as requiring the recipient to enter into Standard Contractual Clauses approved in accordance with Data Protection Laws; or
- Data Protection Laws otherwise permit use to make the transfer.

If you would like more detailed information on the measures and safeguards which we implement for such data transfers, then please contact us using the details set out in section 1 of this statement.

8. YOUR RIGHTS AS A DATA SUBJECT

Data Protection Laws provide you with certain rights in relation to your personal data. These are as follows:

- **The right to access your personal data.** This gives you the right to receive a copy of the personal data we hold about you, subject to certain exemptions.
- **The right to request rectification of your personal data.** This gives you the right to have any incomplete or inaccurate personal data we hold about you corrected.
- **The right to request erasure of your personal data.** This allows you to ask us to delete or remove personal data. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below). In certain circumstances this right may not apply, such as where we have a good, lawful reason to continue using the information in question, and if so we shall inform you of such reasons at the relevant time.
- **The right to object to processing of your personal data.** You can object to us processing your personal data for legitimate interests' purposes. We must then stop processing your data unless we have a strong reason to continue which overrides your objection. If your objection is to direct marketing, we must always stop.
- **The right to restrict how your personal data are used.** You can limit how we use your personal data in certain circumstances. Where this applies, any processing of your personal data (other than storing it) will only be lawful with your consent or where required for legal claims, protecting certain rights or important public interest reasons.
- **The right to have a portable copy or transfer your personal data.** You can ask us to provide you, or (where technically feasible) a third party, with a copy of your personal data in a structured, commonly used, machine-readable format. Note this only applies to personal data which we obtain from you and, using automated means, process on the basis of your consent (which in practice will be rare) or in order to perform a contract with you.
- **The right to withdraw consent.** If we are relying on consent to process your personal data you have the right to withdraw that consent at any time.

Further information on the circumstances in which you may exercise the above rights, and the exemptions to them, can be found on the ICO website (see <https://ico.org.uk/your-data-matters/>).

Responding

We try to respond to all personal data requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. Please also bear in mind that there are exceptions to the rights above and some situations where they do not apply.

We may need to request additional information from you to help us confirm your identity. This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you to clarify your request.

Fees for making a request

You will not normally have to pay a fee to access your personal data (or to exercise any of your other rights). However, we may charge a reasonable fee if your request is unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

How to make a request

If you want to exercise any of the rights described above, please write to Data Protection Requests, I-Environment Investments Limited, The Broadgate Tower, 20 Primrose Street, London, EC2A 2EW or email enquiries@ieiltd.co.uk with the subject heading "Data Protection".

Your right to complain to a supervisory authority

You have the right to complain to the Information Commissioner's Office if you are not satisfied with our response to a data protection request or if you think your personal data has been mishandled. For further information on how to make a complaint, please visit <https://ico.org.uk>.

9. UPDATES TO THIS STATEMENT

We will update this statement from time to time. The current version will always be posted on our website. This statement was last updated on 17 June 2025.