



Privacy Policy

2 Shores Recruitment

Environmental Recruitment Specialists

Last updated: 02/12/2025

Next review: 12 months after issue

1. Introduction and Scope

2 Shores Recruitment (“we”, “us”, “our”), acting as a Data Controller, is committed to protecting your personal data and respecting your privacy. This Privacy Policy explains how we collect, use, store, and protect your information when you interact with us as a candidate, an employer, or a visitor to our website.

By using our services, you agree to the practices described in this policy. We do not offer services to children and do not knowingly collect data relating to anyone under the age of 18.

We never sell or trade personal data to third parties.

2. Contact Details

2 Shores Recruitment is a UK-based partnership specialising in sourcing, screening, and placing candidates within the environmental sector. For the purposes of the UK GDPR, we are the Data Controller of your personal data.

We are registered with the Information Commissioner’s Office (ICO).

- Partnership Address: Tegfan, Top Road, Trefriw, LL27 0JX
- Email: info@2shoresrecruitment.co.uk

Data Protection Lead: We are not required to appoint a formal Data Protection Officer. Our Data Protection Lead oversees data protection compliance, and any questions about this policy or your rights should be addressed to them at the email address provided above.

All data protection queries, concerns, and rights requests are handled by our Data Protection Lead.

3. Personal Data We Collect and Use

We may collect and process the following categories of personal data:

A. Information You Provide Directly (Candidates and Employers)

- **Identity & Contact Data:** Name, home address, email address, and phone number.



- Employment Data: CV, employment and education history, job preferences, salary expectations, interview notes, and right-to-work status.
- Business Contact Data: Contact name, business details, job descriptions, and hiring requirements (for employers).

B. Special Category Data (Sensitive Data)

- Where Special Category Data (such as disability or health information) is provided for the purpose of making reasonable adjustments in the recruitment process, we rely on your explicit consent under Article 9(2)(a) UK GDPR.

C. Information from Third Parties (Article 14 Compliance)

We may receive information from public professional profiles (e.g. LinkedIn), referees you have provided, and publicly accessible CV databases.

Note on Public Sources: Where we obtain your personal data from public sources, we will contact you within a reasonable period (typically within 30 days) to provide this privacy information, as required by Article 14 UK GDPR.

This may include limited personal data obtained from private CV databases where our subscription permits access; you may ask us at any time to confirm which source your data came from.

Where we obtain your personal data from publicly accessible sources (e.g. LinkedIn), we rely on Legitimate Interests to identify and contact potential candidates for relevant roles. We provide Article 14 privacy information within a reasonable period as required under UK GDPR.

We only collect data that is relevant and necessary for the recruitment process.

D. Information Collected Automatically

- Where cookies or analytics are used, this may include IP address, browser type, device type, and basic website usage information.

4. Our Legal Basis and Purpose for Processing

Under the UK GDPR, we must have a lawful basis to process your data.

Category	Purpose of Processing	Legal Basis
Recruitment Services	To source, assess, screen, and place candidates with employers. We only collect data that is relevant and necessary for the recruitment process.	Legitimate Interests (for candidates) and Contract (for engaged employer clients).



Agreement to submit CVs (Specific Consent/Agreement) and Legitimate Interests (in providing service)	To submit a candidate's profile to a named prospective employer.	We always obtain your explicit verbal or written agreement before submitting your CV to any Client. Consent is required for each specific submission.
Special Category Data	Processing volunteered data (e.g. for reasonable adjustments).	Explicit Consent under Article 9(2)(a) UK GDPR.
Compliance	Meeting legal obligations such as HMRC requirements, preventing fraud.	Legal Obligation.

Legitimate Interests Assessment (LIA): Where we rely on Legitimate Interests, we have conducted a Legitimate Interests Assessment (LIA) to ensure our interests do not override your fundamental rights and freedoms.

We do not use automated decision-making or profiling that has a legal or similarly significant effect on you.

You may request a copy of our Legitimate Interests Assessment (LIA) at any time.

5. Who We Share Your Data With

We only share your data where necessary and with appropriate safeguards:

- Prospective Employers: Candidate information is shared only with your prior verbal or written consent or agreement to submit your profile.
- Service Providers: Including our website hosting provider, email systems, secure cloud storage, CRM systems, and IT support providers who act as data processors under written agreements.
- Regulatory or Legal Authorities: Such as HMRC or the ICO, where disclosure is required by law.

Our current data processors include our CRM system, cloud storage provider, email service provider, website host, and IT support services. A full list is available on request. *(Imo note - we may need to create a more detailed separate doc when we know what we're using etc)*

A current list of our data processors is available on request. *(legally required)*



6. Data Retention

We retain personal data only as long as necessary for the purposes described (Storage Limitation).

- **Candidate Data:** Retained for 2 years from the date of our last meaningful contact. Where we are required to collect Right-to-Work or identity verification documents as part of the recruitment process, we retain these records for 2 years after the end of any engagement or assignment, in line with legal and Home Office requirements. After this period, the documents are securely deleted. You may request deletion sooner where allowed by law. You have the right to request data deletion, access to your data, and correction of inaccurate information at any time as specified in the Candidate Terms of Engagement document.
- **Definition of Meaningful Contact:** This includes responding to emails, applying for roles, updating your CV, or otherwise actively engaging with our recruitment services.
- **Employer and Contract Data:** Typically retained for 6 years plus the current year to meet business, accounting, and legal requirements.

You may request deletion at any time; however, some records may need to be retained to meet legal or regulatory obligations.

If you request erasure, we may retain a minimal suppression record to ensure you are not contacted again.

7. International Data Transfers

If we transfer your data outside the UK (e.g. where a service provider is located overseas), we will ensure appropriate safeguards are in place, such as:

- A UK adequacy decision; or
- UK-approved International Data Transfer Agreements (IDTAs) or the UK Addendum to EU Standard Contractual Clauses.

Some of our third-party service providers may operate or store data outside the UK. Where this occurs, we ensure appropriate safeguards are applied as required under UK GDPR.

8. Your Rights Under UK GDPR

You have the following rights regarding your personal data: Right to Access, Right to Rectification, Right to Erasure, Right to Restrict Processing, Right to Object (particularly where we rely on legitimate interests), Right to Data Portability, and the Right to Withdraw Consent.

- To exercise these rights or withdraw consent, contact us at: info@2shoresrecruitment.co.uk.
-



9. Right to Lodge a Complaint

You have the right to lodge a complaint with the UK Information Commissioner's Office (ICO) if you have concerns about how your data is handled. Details can be found on their website: www.ico.org.uk.

We would appreciate the chance to deal with your concerns first, so please contact us directly if possible.

10. Cookies

Our website currently uses only strictly necessary cookies, which are essential for performance and security. These do not require consent under PECR.

- If we introduce analytics or non-essential cookies in future, we will update this policy, provide a compliant cookie consent banner, and rely on consent in accordance with UK GDPR and PECR.
- You can set your browser to block or alert you about cookies, including those considered strictly necessary. However, essential functions of the website may not operate correctly.

11. Security Measures

We use appropriate safeguards to protect your personal data, including:

- Secure digital storage and password protection.
- Access restricted to authorised personnel.
- Encryption where possible.
- Use of reputable service providers with appropriate security compliance.

12. Changes to This Policy

We may update this Privacy Policy from time to time. Any updates will be published on this page with a revised date.
