

ARINITE GDPR PRIVACY POLICY

Last updated: May 2026

Next update due: May 2027

Contents

1. Who we are.....	3
2. Our role.....	3
3. Your rights.....	3
4. Sharing your data	4
5. International transfers.....	4
6. Keeping your data secure	4
7. Automated decision-making.....	5
8. Changes to this notice	5
9. Contact us	5
10. Tell me more.....	5
A. Website visitors.....	5
B. Clients and prospective clients	6
C. Consultants and suppliers	6
D. Job applicants and talent pool.....	7

1. Who we are

Arinite Limited is a health and safety consultancy providing audits, inspections, fire risk assessments, DSE and workstation assessments, training, incident investigation and related advisory services to clients across the UK and internationally.

We are registered with the Information Commissioner's Office (ICO) as a data controller, under number ZB366235. Our registered address is:

Arinite Limited

Warnford Court, 29 Throgmorton Street, London EC2N 2AT

Data Protection contact: DPO@arinite.com

2. Our role

Arinite acts in two capacities depending on the context:

- **As a Controller** – when we process personal data for our own internal business purposes, such as managing client relationships, engaging consultants, recruiting and handling enquiries. This Privacy Notice covers these activities.
- **As a Processor** – when we process personal data on behalf of our clients during the delivery of health and safety services (for example, storing DSE assessments or accident reports in our systems on a client's instruction). In those cases, the client is the Controller, and their own privacy notice will apply to the individuals whose data is involved.

This Privacy Notice covers only the activities where Arinite acts as Controller. It does not cover employee and worker data, which is addressed in a separate Employee Privacy Notice.

3. Your rights

You have rights in respect of our processing of your personal data. Subject to certain conditions, these are:

- Right to be informed – to be told about how and why we collect and use your personal data (which is the purpose of this notice).
- Right of access – to request a copy of the personal data we hold about you and details of how we use it.
- Right to rectification – to ask us to correct any inaccurate or incomplete personal data we hold about you.
- Right to erasure – to ask us to delete your personal data where there is no compelling reason for us to continue holding it.
- Right to restriction – to ask us to pause processing your personal data in certain circumstances, for example whilst we verify its accuracy.
- Right to object – to ask us to stop processing your personal data where we are relying on legitimate interests as our lawful basis, if something about your particular situation gives you grounds to object.
- Right to data portability – in certain circumstances, to request that we transfer your data to you or another organisation in a structured, commonly used, machine-readable format.
- Right not to be subject to automated decision-making, using special category data – to object to decisions being made about you solely by automated means without human involvement.

To exercise any of these rights, please contact us at DPO@arinite.com.

If you are not satisfied with how we handle your data or your request, you have the right to lodge a complaint with the Information Commissioner's Office (ICO). Please note, prior to lodging a complaint with the ICO please contact Arinite using DPO@arinite.com.

Arinite will acknowledge your complaint within the statutory timeframe of 30 days and attempt to resolve your complaint at the earliest opportunity.

If you remain unsatisfied with our response, you are able to lodge a complaint with the ICO via the following link:

<https://ico.org.uk/make-a-complaint/>

4. Sharing your data

We only share personal data where it is necessary and proportionate. We may share data with:

- Service providers and processors – companies that provide tools and services we rely on (see the notices below for specifics by audience type). We have Data Processing Agreements in place with all processors.
- Professional advisers – accountants, lawyers and auditors where required.
- Statutory and regulatory bodies – where we are legally required to disclose information, for example HMRC or the ICO.
- Prospective buyers – if Arinite is involved in a merger, acquisition or sale, personal data may be transferred as part of that transaction. We will notify you in advance if this happens.

We never sell personal data to third parties.

5. International transfers

Some of the tools and systems we use are hosted or operated by companies based outside the UK or EEA. Where personal data is transferred internationally, we ensure appropriate safeguards are in place. These may include:

- Adequacy decisions – where the destination country has been recognised by the UK as providing an equivalent level of data protection.
- Standard Contractual Clauses (SCCs) and/or the UK International Data Transfer Agreement (IDTA) – contractual safeguards approved for use in international transfers.

We carry out due diligence and transfer impact assessments where appropriate to ensure your data remains protected. The specific tools that may involve international transfers are identified in the audience-specific notices below.

6. Keeping your data secure

Arinite takes the security of your personal data seriously. We have put in place appropriate technical and organisational measures to protect your data against accidental loss, unauthorised access, alteration or disclosure. These include:

- Access controls limiting who can view personal data to those with a business need.
- Secure cloud-based systems with encryption in transit and at rest.
- Confidentiality obligations on all staff and contractors.
- Procedures for detecting, reporting and investigating data breaches.

Where we share data with processors and other third parties, we require them to implement equivalent security measures and to process data only in accordance with our instructions.

7. Automated decision-making

We do not use your personal data in any automated process to make decisions about you that produce legal or similarly significant effects without human involvement.

8. Changes to this notice

We may update this Privacy Notice from time to time, for example if our processing activities change or if there are updates to the law. When we make significant changes, we will publish an updated version on our website and, where appropriate, contact you directly to let you know.

The date at the top of this notice shows when it was last reviewed.

9. Contact us

If you have any questions about this notice or about how we handle your personal data, please contact our Data Protection contact at DPO@arinite.com or write to us at the address in section 1.

10. Tell me more...

Select the section below that best describes your relationship with Arinite for details of the specific data we hold about you and why.

- Website visitors
- Clients and prospective clients
- Consultants and suppliers
- Job applicants and talent pool

A. Website visitors

This section applies if you visit the Arinite website (www.arinite.com).

Data we collect

When you visit our website, we may automatically collect the following:

- IP address and general location
- Browser type, device type and operating system
- Pages visited, time on site and referring URL
- Cookie identifiers where cookies are in use

How and why we use it

We use this data to ensure the website functions correctly (essential cookies and technical operations) and, where you have consented, to understand how visitors use the site so that we can improve it.

Lawful basis

- Legitimate interests – for essential technical functionality (no consent required).
- Consent – for any analytics or non-essential cookies. You can manage your preferences via the cookie banner when you first visit the site.

Retention

Website usage data is retained for up to 14 months.

B. Clients and prospective clients

This section applies if you are a contact at an existing or prospective Arinite client organisation, or if you have previously engaged with Arinite's sales and marketing activities (including the legacy SafeHands mailing list).

Data we collect

Depending on your relationship with us, we may hold the following:

- Contact details: first name, last name, email address, telephone number
- Company details: company name, address, website URL, industry sector
- Commercial information: client terms of reference, contract details, P&L information
- Communications: notes of conversations, emails and meeting records
- CRM data: records in HubSpot and Apollo including interaction history and lead status
- Marketing preference data: email address and opt-in/opt-out status (for legacy SafeHands newsletter subscribers)

How and why we use it

We use this data to:

- Manage our client relationships and deliver contracted services
- Send proposals, contracts and invoices
- Maintain our CRM system and client records
- Communicate with you about our services, including by email
- Re-market to legacy SafeHands newsletter subscribers who have previously opted in

Where we get your data

We receive most data directly from you. For prospective client leads, some contact details (such as name, job title and email address) may be sourced from LinkedIn or via third-party tools such as Apollo or InstantlyAI.

For the SafeHands legacy list, data was collected via an opt-in process at the time of the SafeHands service. If you no longer wish to receive communications, you can unsubscribe at any time using the link in any of our emails or by contacting us at

DPO@arinite.com.

Lawful basis

- Legitimate interests – to manage our commercial relationships, prospect for new business (where you are a corporate contact) and maintain our CRM records. To fulfil our obligations to you or your organisation, including issuing invoices and managing service delivery. We have assessed that this does not override your interests or rights.
- We also rely on the business-to-business soft opt-in provisions under PECR for direct marketing communications.

Retention

- Client contract and billing records: 7 years from the end of the contract (for legal and tax purposes).
- CRM and relationship management data: 6 years from the end of our relationship.
- Prospecting and lead data: up to 2 years from the last relevant interaction, or until you unsubscribe.
- SafeHands newsletter data: until you unsubscribe or ask us to delete it.

C. Consultants and suppliers

This section applies if you are an independent consultant engaged by Arinite to deliver health and safety services, or a contact at a supplier organisation.

Data we collect

- Contact details: name, email address, telephone number, country of operation
- Professional details: qualifications, accreditations, specialist skills and areas of expertise
- Identity and compliance documents: professional indemnity insurance evidence, right to work documentation
- Contractual documents: signed contracts, NDAs and associated correspondence
- Arinite CV: a company-formatted CV used for client-facing purposes
- LinkedIn profile details: used to verify qualifications and credentials
- Work records: projects and reports you have authored or contributed to, client point-of-contact names included in those reports
- Financial details: invoices, bank account details for payment
- Communications: email correspondence and meeting records

How and why we use it

We use this data to:

- Onboard you as a consultant, including issuing contracts and NDAs
- Maintain a directory of active consultants and allocate work
- Verify that you hold the necessary qualifications and insurance
- Assign projects and share relevant templates and briefing materials
- Receive your completed reports and deliverables
- Process your invoices and make payments

Lawful basis

- Contract, if you are an individual, and Legitimate interest if you are an employee for a contracting entity– for onboarding, contracting, work allocation and payment. This data is necessary to perform or prepare for a contract with you.
- Legitimate interests – for maintaining the consultant directory, verifying qualifications and managing the ongoing relationship. Our legitimate interest is in running an effective and compliant network of qualified consultants.

Retention

- Contract and payment records: 7 years from the end of the engagement (for legal and tax purposes).
- Consultant directory and qualification records: for the duration of the engagement and up to 2 years after, to facilitate re-engagement.
- Work records and reports: as long as required for the relevant client project, typically 7 years.

D. Job applicants and talent pool

This section applies if you have applied for a role with Arinite or have given consent for us to retain your details for future opportunities.

Note: if your application is successful and you join Arinite as an employee, a separate Employee Privacy Notice will be provided to you on commencement.

Data we collect

During the recruitment process, we may collect and process the following:

- Contact details: name, email address, telephone number, address
- CV, cover letter and application information
- Interview notes and assessments
- Information about your current or previous salary and benefits
- Professional qualifications and memberships
- Right to work documentation (e.g. passport or visa)
- References from current or previous employers
- Background check information, including qualifications verification and — where relevant for the role — criminal records checks via the Disclosure and Barring Service (DBS)
- Social media profile information (e.g. LinkedIn) used in candidate sourcing or screening

Special category data

Where relevant to the role or required by law, we may also process special category data, including information about health or disability (for reasonable adjustments purposes) and, in limited circumstances, information about criminal convictions. We will only process such data where we have a specific legal basis to do so under the UK GDPR and the DPA 2018.

How and why we use it

We use this data to:

- Manage and assess applications for employment
- Conduct interviews and make hiring decisions
- Carry out background and reference checks prior to an offer being made
- Comply with our legal obligations, including right-to-work checks
- Fulfil our duty to make reasonable adjustments for candidates with disabilities

Where we get your data

We collect most data directly from you. We may also receive information from recruitment platforms (such as Indeed or LinkedIn), employment agencies and — once a conditional offer has been made — from referees and background check providers. We will inform you when we seek information from these third-party sources.

Lawful basis

- Pre-contractual steps / Contract – processing your application and taking steps to enter into a contract of employment with you.
- Legal obligation – checking your right to work in the UK and complying with employment law obligations.
- Legitimate interests – managing the recruitment process, conducting due diligence on prospective staff and defending legal claims.
- Consent – for retaining your details in our talent pool if your application is unsuccessful (see below).
- DPA 2018, Schedule 1 conditions – for processing health information and criminal records data where required for employment law purposes.

Retention

- Unsuccessful applicants: we will retain your data for up to 6 months following the end of the relevant recruitment exercise, after which it will be securely deleted.

- Talent pool: if you consent to us retaining your details for future opportunities, we will hold your CV, name and contact details for up to 12 months from the date of your application. You can withdraw consent and ask us to delete your data at any time.
- Successful applicants: data gathered during recruitment will be retained as part of your employment record in accordance with the Employee Privacy Notice.

If your application is unsuccessful and you would like us to consider you for future roles, we will ask for your explicit consent before retaining your details. You can withdraw that consent at any time by contacting us at DPO@arinite.com.