

# Privacy Policy

## WHO WE ARE

Calcot Asbestos Recruitment Limited, (referred to in these terms of use as “CALCOT”, “we”, “us”, “or “our”) Calcot is a limited liability company registered in England and Wales with company registration number 08985227 and our registered office address located at 5 Theale Lakes Business Park, Moulden Way, Sulhamstead, Reading, Berkshire, RG7 4GB, United Kingdom

Calcot Asbestos Recruitment Ltd are registered with the UK Information Commissioner's Office (“ICO”) under registration number ZA106765.

## CONTACTING US

Calcot Asbestos Recruitment are not required to appoint a formal data protection officer under data protection laws. However, we have appointed an internal company representative who will deal with all aspects of privacy and may be contacted in relation to any queries you may have in relation to this Privacy Policy or more details on your data held by us. You can contact Stephen at [privacy@calcotasbestosrecruitment.co.uk](mailto:privacy@calcotasbestosrecruitment.co.uk)

If you have any questions about our privacy policy or your information, or to exercise any of your rights as described in this privacy policy or under data protection laws, you can also contact us:

By post:

Privacy Manager, Steve Lee

Unit 5, Theale Lakes Business Park,

Moulden Way, Sulhamstead,

Reading, Berkshire RG7 4GB

United Kingdom

By telephone: + 44 (0) 1189 421 231

By email: [privacy@calcotasbestosrecruitment.co.uk](mailto:privacy@calcotasbestosrecruitment.co.uk)

## PERSONAL DATA

Definition: ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

## DATA PROTECTION PRINCIPLES

Calcot Abestos Recruitment adheres to the following GDPR principles when processing your personal data:

1. **Lawfulness, fairness and transparency** – data must be processed lawfully, fairly and in a transparent manner.
2. **Purpose limitation** - data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. **Data minimisation** - data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy** - data must be accurate and, where necessary, kept up to date.
5. **Storage limitation** - data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

6. **Integrity and confidentiality** - data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage by using appropriate technical or organisational measures.

## What are your rights and how can you exercise them?

You may exercise the following rights under the conditions and within the limits set forth in the law:

- the right to access your personal data as processed by us and, if you believe that any information relating to you is incorrect, obsolete or incomplete, to request its correction or updating;
- the right to request the erasure of your personal data or the restriction thereof to specific categories of processing;
- the right to withdraw your consent at any time, without affecting the lawfulness of the processing before such withdrawal;
- the right to object, in whole or in part, to the processing of your personal data; and
- the right to request its portability, i.e. that the personal data you have provided to us be returned to you or transferred to the person of your choice, in a structured, commonly used and machine-readable format without hindrance from us and subject to your confidentiality obligations.
- You can exercise any of your rights as described in this Privacy Policy and under data protection laws by contacting us as provided in "Contacting us" above.
- Save as described in this Privacy Policy or provided under data protection laws, there is no charge for the exercise of your legal rights. However, if your requests are manifestly unfounded or excessive, in particular because of their repetitive character, we may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or taking the action requested; or (b) refuse to act on the request.
- Where we have reasonable doubts concerning the identity of the person making the request, we may request additional information necessary to confirm your identity.

## RESPONSIBILITY OF THE CONTROLLER

Calcot being a data controller and taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, we shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the General Data Protection regulation (GDPR). Those measures shall be reviewed and updated where necessary.

1. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
2. Adherence to approved codes of conduct or approved certification mechanisms may be used as an element by which to demonstrate compliance with the obligations of the controller.

## OUR PRIVACY PROMISE

**Transparency** – We will always tell you what data we're collecting about you and how we use it. We only share your data with trusted partners and will never sell your data.

**Secure** – We are committed to always follow industry best practices to ensure your data is stored safely and securely. We protect the confidentiality, accuracy and availability of the information we collect about you.

**Control** – We will always give you control over the marketing you receive from us. You can choose the types of messages you receive and whether you want to stop receiving any marketing communications.

## Legal basis for the processing

If any legal basis for processing needs to be changed or updated over time, or if we have a new purpose which we did not originally anticipate, we will update this section as long as new purpose is compatible with the original purpose.

## The lawful bases for processing

The lawful bases for processing are set out in Article 6 of the GDPR.

- (a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- (b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- (d) Vital interests:** the processing is necessary to protect someone's life.
- (e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

We will not process your personal data if we do not have a proper justification foreseen in the law for that purpose. Therefore, we will only process your personal data if:

- I. we have obtained your prior consent to collect your data;
- II. the processing is necessary to perform our contractual obligations towards you or to take pre-contractual steps at your request;
- III. the processing is necessary to comply with our legal or regulatory obligations; or
- IV. the processing is necessary for our legitimate interests and does not unduly affect your interests or fundamental rights and freedoms.

Please note that, when processing your personal data on this last basis, we always seek to maintain a balance between our legitimate interests and your privacy. Examples of such 'legitimate interests' are data processing activities performed:

- to benefit from cost-effective services (e.g. we may opt to use certain platforms offered by suppliers to process data);
- to offer our products and services to our customers;
- to prevent fraud or criminal activity, misuses of our products or services as well as the security of our IT systems, architecture and networks;
- to sell any part of our business or its assets or to enable the acquisition of all or part of our business or assets by a third party; and
- to meet our corporate and social responsibility objectives.

## Purposes of the processing of data

We always process your personal data for a specific purpose and only process the personal data which is relevant to achieve that purpose. In particular, we process your personal data for the following purposes:

- for the purposes of our employees, clients and to manage our third party suppliers and service providers;
- organise tender-offers (if applicable), implement tasks in preparation of or to perform existing contracts;

- monitor activities at our facilities, including compliance with applicable policies as well as health and safety rules in place;
- grant you access to our training modules allowing you to provide us with certain services;
- manage our IT resources, including infrastructure management and business continuity;
- preserve the company's economic interests and ensure compliance and reporting (such as complying with our policies and local legal requirements, tax and deductions, managing alleged cases of misconduct or fraud, conducting audits and defending litigation);
- manage mergers and acquisitions involving our company if applicable;
- archiving and record-keeping;
- billing and invoicing; and
- any other purposes imposed by law and authorities.

### **Who has access to your personal data and who are they transferred to?**

Calcot holds your data and we will not sell, share, or otherwise transfer your personal data to any other third parties other than those indicated in this Privacy Notice without your prior consent to do so.

In the course of our activities and for the same purposes as those listed in this Privacy Notice, your personal data can be accessed by or transferred to the following categories of recipients on a need to know basis to achieve such purposes:

- our personnel (mainly financial and HR and sometimes other departments within Calcot Asbestos Recruitment);
- our independent agents or brokers (if any or applicable);
- our other suppliers and services providers that provide services and products to us;
- our IT systems providers, cloud service providers and consultants;
- any third party to whom we assign or novate any of our rights or obligations; and
- our advisors and external lawyers in the context of the sale or transfer of any part of our business or its assets.

The above third parties are contractually obliged to protect the confidentiality and security of your personal data, in compliance with applicable law.

**Your personal data can also be accessed by or transferred to any national and/or international regulatory, enforcement, public body or court, where we are required to do so by applicable law or regulation or at their request.**

The personal data we collect from you may also be processed, accessed or stored in a country outside the UK, which may not offer the same level of protection of personal data.

If in the case we are required to transfer any of your personal data to external companies, legal entities in other jurisdictions, we will make sure to protect your personal data by applying the level of protection that is required under the local data protection/privacy laws applicable to the UK, acting in accordance with our policies and standards and, for entities located in the European Economic Area (i.e. the EU Member States plus Iceland, Liechtenstein and Norway, the "EEA"), unless otherwise specified, only transferring your personal data on the basis of standard contractual clauses approved by the European Commission. You may request additional information in relation to international transfers of personal data and obtain a copy of the adequate safeguard put in place by exercising your rights.

## Personal data we collect

We collect and process the following personal data from you:

- **Identity and Contact Data**, including your business details, name, address, telephone number, date of birth, marital status, passport number, employment history, educational or professional background, tax status, employee number, job title and function, and other personal data concerning your preferences relevant to our services;
- **Financial and Payment Data**, including your bank account and other data necessary for processing payments and fraud prevention, including credit/debit card numbers, security code numbers and other related billing information;
- Business Information, including information provided in the course of the contractual or client relationship between you or your organisation and Calcot, or otherwise voluntarily provided by you or your organisation;
- **Profile and Usage Data**, including passwords if applicable to Calcot website(s) or in the case of password protected platforms or services, your preferences in receiving marketing information from us, your communication preferences and information about how you use our websites(s) including the services you viewed or searched for, page response times, download errors, length of visits and page interaction information (such as scrolling, clicks, and mouse-overs). To learn more about our use of cookies or similar technology please check our cookies policy [here](#);
- **Technical Data**, including information collected during your visits to our website(s), the Internet Protocol (IP) address, login data, browser type and version, device type, time zone setting, browser plug-in types and versions, operating system and platform. To learn more about our use of cookies or similar technology please check our cookies policy [here](#);
- Physical Access Data, relating to details of your visits to our premises;
- Sensitive personal data: In the course of our client services, we may be required to collect and use sensitive personal information relating to you (that is, information about your racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life and sexual orientation or details of criminal offences, or genetic or biometric data).

For example, we may need to hold information about medical conditions, race, religion and/or sexual orientation may be relevant to the representation. Similarly, we may need to collect sensitive personal information on tax or social security matters. Where we process sensitive personal information in the course of these and other similar services for clients, suppliers and or employees, we do so to assist you and/or your organisation to establish, or to assist you and/or your organisation in fulfilling the rights and obligations of applicable employment or social security laws.

**Under the GDPR, an employee, client, supplier or third-party provider has a right to be informed of:**

- what records/data are kept by us, the lawful basis of the collection and usage and who they are shared with;
- the confidentiality and the security of the records we hold;
- in the case of our employees, how these records can help with their training and development at work;

## Information to be provided where personal data are collected from the data subject

Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

1. the identity and the contact details of the controller and, where applicable, of the controller's representative;
2. the contact details of the data protection officer, where applicable;
3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4. where the processing is based on point (f) of [Article 6\(1\)](#), the legitimate interests pursued by the controller or by a third party;
5. the recipients or categories of recipients of the personal data, if any;
6. where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in [Article 46](#) or [47](#), or the second subparagraph of [Article 49\(1\)](#), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

## HOW LONG WE KEEP YOUR PERSONAL DATA

**We will only keep your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.**

At the end of that retention period, your data will either be deleted or anonymised (so that it can no longer be associated with you) for research or statistical purposes.

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 unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances you may be entitled to ask us to delete your data: see your rights below for further information.

The criteria we use for retaining different types of personal data, includes the following:

- **General queries** - when you make an enquiry or contact us by email or telephone, we will retain your information for as long as necessary to respond to your queries. After this period, we will not hold your personal data for longer than one year if we have not had any active subsequent contact with you;
- **Direct marketing** - where we hold your personal data on our database for direct marketing purposes (if applicable), we will retain your information for no longer than two years if we have not had any active subsequent contact with you.
- **Legal and regulatory requirements** - we may need to retain personal data for up to 7 years after we cease providing services and products to you where necessary to comply with our legal obligations, resolve disputes or enforce our terms and conditions.

## CHILDREN

Our website and business operations is not intended for or directed at children under the age of 16 years and we do not knowingly collect data relating to children under this age.

## EMAIL MARKETING

For email marketing to an individual subscriber (that is, a non-corporate email address) with whom we have not previously engaged as a client, we need your consent to send you any unsolicited email marketing.

Where you do provide consent, you can withdraw your consent at any time, but without affecting the lawfulness of processing based on consent before its withdrawal.

You have the right to opt out of receiving email marketing communications from us at any time by:

- contacting our [Privacy Manager](#) using the contact details set out above; or
- using the “unsubscribe” link in emails.

## INTERNATIONAL TRANSFERS

We do not transfer any personal data outside the UK or the European Economic Area (EEA).

## SECURITY OF YOUR PERSONAL DATA

Calcot have implemented appropriate technical and organisational controls to protect your personal data against unauthorised processing and against accidental loss, damage or destruction. You are responsible for choosing a secure password when we ask you to set up a password to access parts of our sites or apps. You should keep this password confidential and you should choose a password that you do not use on any other site. You should not share your password with anyone else, including anyone who works for us. Unfortunately, sending information via the internet is not completely secure. Although we will do our best to protect your personal data once with us, we cannot guarantee the security of any personal data sent to our site while still in transit and so you provide it at your own risk.

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of

natural persons, we, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

1. the pseudonymisation and encryption of personal data where applicable;
  2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
  4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
  3. Adherence to an approved code of conduct or an approved certification mechanism may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1.
  4. We the controller shall take steps to ensure that any natural person acting under the authority of the controller who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

We use industry standard physical and procedural security measures via our third-party provider to protect information from the point of collection to the point of destruction. This includes encryption, firewalls, access controls, policies and other procedures to protect information from unauthorised access.

Where data processing is carried out on our behalf by a third party provider, we take steps to ensure that appropriate security measures are in place to prevent unauthorised disclosure of personal data.

Despite these precautions, however, Calcot cannot guarantee the security of information transmitted over the Internet or that unauthorised persons will not obtain access to personal data.

## COOKIES

In order to improve our website, we may use small files commonly known as “cookies”. A cookie is a small amount of data which often includes a unique identifier that is sent to your computer or mobile phone (your “**device**”) from our website and is stored on your device’s browser or hard drive. The cookies we use on our website won’t collect personally identifiable information about you and we won’t disclose information stored in cookies that we place on your device to third parties.

By continuing to browse our website, you are agreeing to our use of cookies.

If you don't want us to use cookies when you use our website, you can set your internet browser not to accept cookies. However, if you block cookies some of the features on our website may not function as a result.

You can find more information about how to do manage cookies for all the commonly used internet browsers by visiting [www.allaboutcookies.org](http://www.allaboutcookies.org). This website will also explain how you can delete cookies which are already stored on your device.

## LINKS

Our website may, from time to time, contain links to and from third-party websites. If you follow a link to any of these websites, please note that these websites have their own privacy policies and Calcot does not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

## DATA BREACHES

In the event of a data breach, Calcot have put in place and recorded procedures within the scope of the GDPR to deal with any suspected breach and will notify you and any applicable regulator of a breach where required to do so.

## The Privacy and Electronic Communications Regulations (PECR)

Calcot adhere to the Privacy and Electronic Communications Regulations (PECR) sit alongside the previous Data Protection Act 1998 and the current GDPR. They give people specific privacy rights in relation to electronic communications.

There are specific rules on: marketing calls, emails, texts and faxes; cookies (and similar technologies); keeping communications services secure; and customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

We will, under the GDPR, abide under these rules to insure compliance is met.

## EMAIL & MONITORING

Whilst every member of the Calcot team has a personal private email address and has regular training in email usage and its appropriate security, emails that you send to us or which we send to you may be monitored for security and to ensure compliance with professional standards and our internal compliance policies. Monitoring is not continuous or routine, but under the GDPR, this may be undertaken to insure the compliance of company emailing is in line with compliance procedures and standards. Occasional spot checks or audits may also be undertaken to insure its ongoing compliance.

## COMPLAINTS

If you have any questions or complaints regarding our Privacy Policy or practices, please contact us as provided in "Contacting Us" above.

You have the right to make a complaint at any time with a supervisory authority, in particular in the EU (or EEA) state where you work, normally live or where any alleged infringement of data protection laws occurred. **The supervisory authority in the UK is ICO who can be contacted at <https://ico.org.uk> or telephone on 0303 123 1113.**

## CHANGES TO OUR PRIVACY POLICY

From time to time, we may need to change or update this Privacy Policy. The current version of this Policy will always be available from us in hard copy or on our website. We will post a prominent notice on our website to notify you of any significant changes to this Policy or update you by other appropriate means.

This Private Policy has been updated and effective as of

**May 24, 2018.**

Our Privacy Policy has been independently quality assured by JVR Consultancy [JVR Consultancy](#)