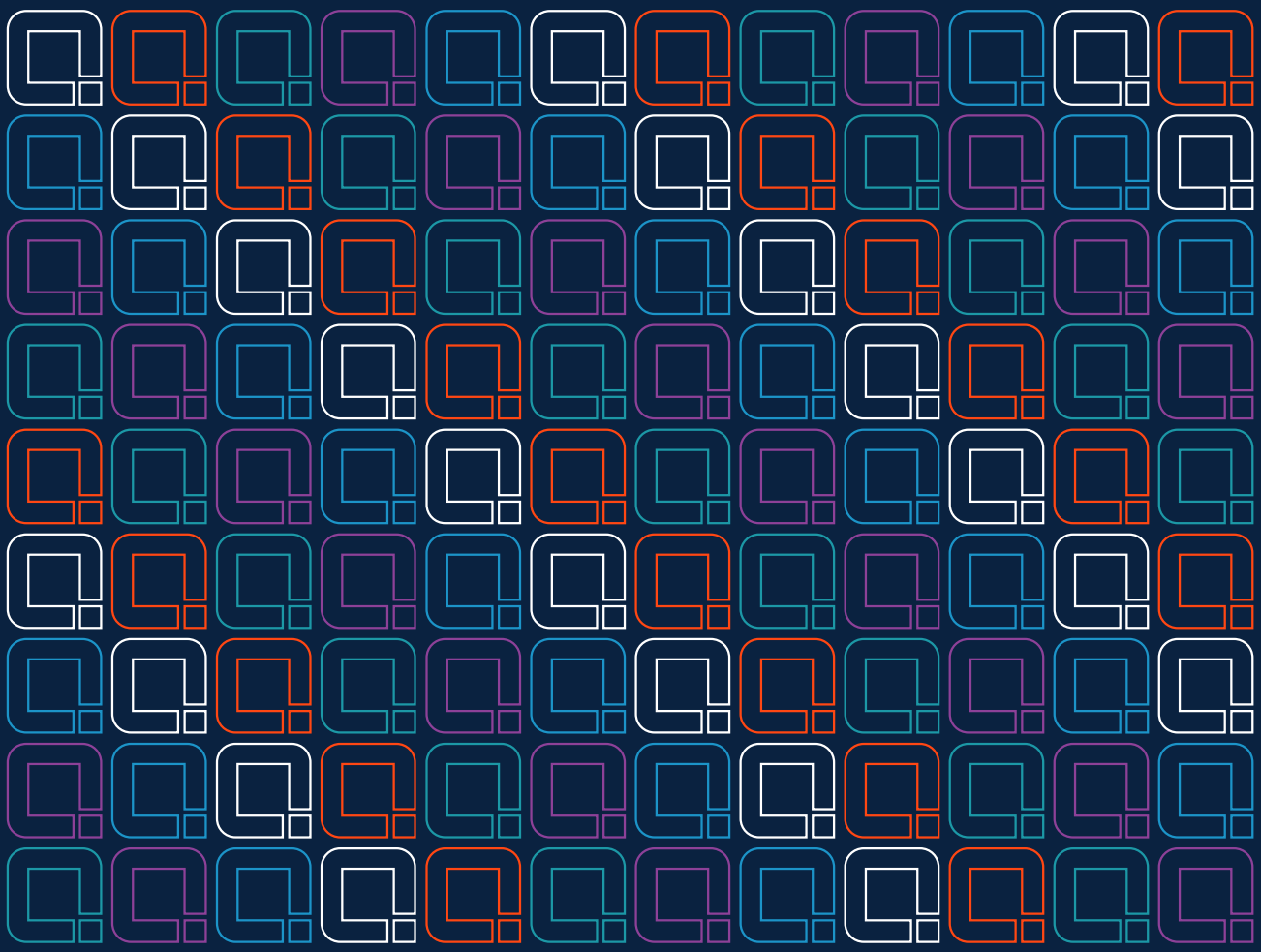
quadmark

Advise ▪ Create ▪ Enable

Privacy Statement



Quadmark Privacy Statement

This Privacy Statement sets out the basis on which we use personal data in respect of our recruitment process.

Definitions:

- **Data Protection Legislation** means (i) the General Data Protection Regulation ((EU) 2016/679), the Data Protection Act 2018, and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 2018.
- **Applicant** means a person who has submitted an application or enquiry, directly or indirectly, with a view to becoming an Employee.

1. How We Obtain Personal Data

If you are a **Applicant**, we may obtain personal data relating to you:

Directly if you have:

- Applied for an open role through our website.
- Sent your CV directly to us.
- Attended an interview or assessment day with us.

Indirectly from:

- Third-party recruitment businesses.
- Job boards and CV search databases, such as Total Jobs and Indeed.
- Professional networking sites, such as LinkedIn.
- Third-party references.
- Individuals who have recommended you to us.

2. Types of Information We Hold

If you are an **Applicant**, we may collect, store, and process the following types of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and email addresses.
- Your gender, date of birth, marital status, and nationality.
- Proof of your right to work in the United Kingdom such as copies of your passport and, where applicable, visa, residence permit, or similar government documents.
- Proof of your identity and address.
- Your qualifications and certifications.
- Any information within your CV, cover letter, and application form.
- Any other information captured during the recruitment process.
- Academic, professional, and personal references from third parties.

If you are an **Applicant** we may also collect, store, and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation, and political opinions.
- Trade union membership.
- Information about your health, including any medical condition, disability, health, and sickness records
- Information about criminal convictions and offences.

3. How We Use Personal Data

If you are an **Applicant**, we may use your personal data to:

- Make a decision about your appointment or engagement.
- Determine the basis on which you may be employed or engaged by us, where applicable.
- Check that you are legally entitled to work in the United Kingdom.
- Verify the information which you have provided during the recruitment process.
- Carry out data analysis into Applicant attraction and conversion.
- Carry out Equal Opportunities monitoring.

4. Our Lawful Basis for Processing Data

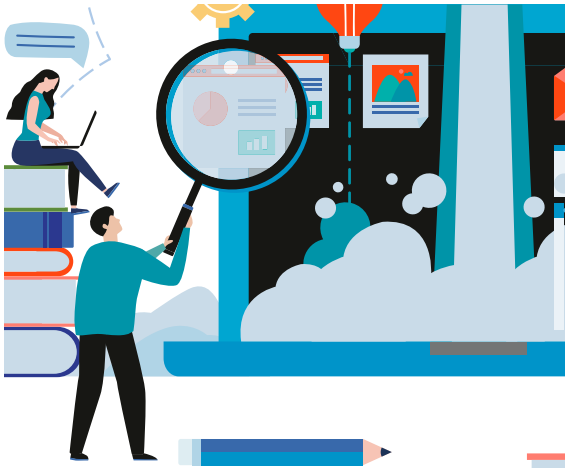
We are entitled to process your personal data where it is necessary for the performance of the contract for services or contract of service to which you are a party, either directly with us or, in some circumstances, with a third party. This includes any processing which may be necessary at the preliminary stage prior to you entering into a contract, provided that this is done at your request e.g. by submitting an application.

We may also process your personal data where it is necessary for compliance with a legal obligation to which we are subject, such as the obligation to maintain suitable business and financial records.

In accordance with Article 9 (2)(b) of the GDPR, we are entitled to process your sensitive personal data where we need to carry out our obligations or exercise our rights in the field of employment. Under very limited circumstances, we may also ask for consent to process your sensitive personal data.

5. Where We Process Personal Data

Quadmark operates in the UK, Luxembourg, the US and Singapore, and uses service providers based around the world. Consequently, your personal data may be processed in countries outside of Europe, including in countries where you may have fewer legal rights in respect of your information than you do under local law. If we transfer personal data outside the European Economic Area or the UK we will, as required by applicable law, ensure that your personal data is protected by appropriate safeguards. Please contact us if you would like more information about these safeguards.



6. How do we store the Data

We use Google Suite applications which offer not only an enhanced level of management and resilience for business continuity, but also for data security, ensuring the data we hold is held securely with the most recent updates applied to prevent data breaches.

7. Parties with Whom We May Share Data

We may share your personal data for legitimate purposes with:

- Our directors, officers, and employees where it is appropriate and necessary to do so.
- Our connected or associated companies.
- Where applicable, any third-party company through which you are contracting.
- Third-Party Services Providers including Shipleys, our payroll and HR operations provider.
- Any third-party who you have engaged and to whom you have confirmed that we may provide personal data, such as your bank or mortgage advisor.
- Our clients, where it is reasonable and necessary to do so e.g. where we provide your business contact information or, in the event of a dispute, provide internal communications or explanations as to the actions which you have taken.
- Any third party to which we may be planning to transfer or sell a relevant part of our business.
- Governmental departments and agencies where we are permitted or required by law to do so.

If we share your information with any third party, we will require them to respect your data privacy and only use your data for the purpose for which it was provided or otherwise as permitted by law.

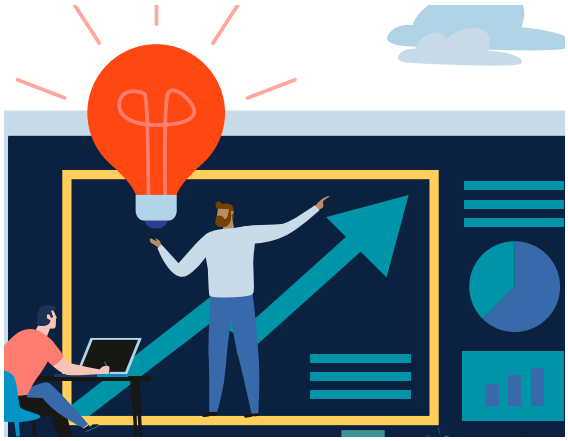
8. Automated Decision-Making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. All decisions which are made in the course of our business processes involve human intervention. We do not make any decisions about you using automated means but will let you know if this changes.

9. Data Security

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used, or accessed in an unauthorised way, altered, or disclosed. In addition, we limit access to your personal information to those employees, contractors, and other third parties who have a business “need to know”. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.



10. Data Retention

We will only retain your personal information 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. 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.

If you are an **Applicant**, we will usually retain your personal data for one year from the date on which the recruitment decision is made, unless you become an **Employee**, in which case the provisions below shall apply.

If you are an **Employee**, we retain your data (i) for auditing or compliance purposes (ii) in respect of any potential or actual legal proceedings and (iii) to comply with our obligations to HMRC. We will therefore keep your data for up to seven years from the date on which our working relationship ends, although any data which is no longer required for any purpose and which should be deleted for data security reasons (such as your personal bank details) will be deleted from our records on the termination of our working relationship.

In some circumstances, we may completely anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

11. Rights of access, correction, erasure, and restriction

Your duty to inform us of changes. It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information. Under certain circumstances, you have the right to:

- Request **access** to your personal information (Subject Access Request). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it. You will not usually have to pay a fee to access your personal information, but we may charge a reasonable fee if your request is clearly unfounded, repetitive, or excessive. Alternatively, we may refuse to comply with the request in such circumstances.
- Request **correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request **erasure** of your personal information. This enables you to ask us to delete or remove personal information where the personal data is no longer necessary to the purpose for which it was originally collected/ processed, or you have objected to the processing, and there is no overriding legitimate interest for continuing the processing.
- **Object** to the processing of your personal information where we are relying on a legitimate interest and you object on “grounds relating to your particular situation.”

- Request the **restriction** of processing your personal information. This enables you to ask us to block or suppress the processing of personal information about you, for example, if you want us to establish its accuracy or the reason for processing it or if you have also objected to the processing as above.
- Request the **transfer** of your personal information to another party when the processing is based on consent and carried out by automated means. This right is not usually applicable to any data processing carried out by Quadmark.

If you want to exercise any of the above rights, please contact the UK General Manager in writing. We will consider your request and confirm the actions which we have taken in response to such request.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is an appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

In the limited circumstances where you may have provided your consent to the collection, processing, and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time.
To withdraw your consent, please contact the UK General Manager. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law. We will confirm the actions which we have taken in respect of any such request.

If you are unhappy with any aspect of the manner in which we have processed your personal data or dealt with your decision to exercise any of the rights set out in this section, you have the right to complain to the Information Commissioner's Office in the United Kingdom. Their details are:

Information Commissioner's Office,
Wycliffe House, Water Lane, Wilmslow,
Cheshire SK9 5AF
Tel: 0303 123 1113 (local rate) or, if you prefer to use a national rate number, 01625 545 745
Email: casework@ico.org.uk

12. Contacting Us

If you have any questions about our Privacy Statement, you can speak to your line manager (where applicable) or contact the UK General Manager.