

Privacy Notice

Introduction

Swift Strategies Limited respects your privacy and is committed to protecting your personal data. This privacy notice tells you how we look after your personal data when you interact with us and it tells you about your privacy rights and how the law protects you. We may update this Notice at any time and will inform you of any changes.

Important information

This privacy notice is issued on behalf of Swift Strategies Limited so when we mention “Swift Strategies”, “we”, “us” or “our” in this privacy notice, we are referring to Swift Strategies Limited as responsible for processing your data. For the purposes of the Data Protection Legislation, Swift Strategies is a “controller” in relation to your personal information. This means that Swift Strategies is responsible for deciding what your personal information is used for by Swift Strategies (and its processors), and how it is used. Swift Strategies is required under Data Protection Legislation to provide you with the information contained in this notice. Our full details are:

Company name:	Swift Strategies Limited
Registered address:	Second Floor, 150 Fleet Street London EC4A 2DQ
Contact email address:	info@swiftstrategies.co.uk
Data protection contact:	Nathan Swift, nathan.swift@swiftstrategies.co.uk

This privacy notice gives you information about how we collect and use personal data before, during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR).

Changes to the Privacy Notice and your duty to inform us of changes.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

The type of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We will collect, store and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, date of birth, telephone numbers, and personal email addresses
- Next of kin and emergency contact information
- Bank account details
- Right to Work screening data, including scans/copies of the following; Passport, Proof of Address, Work Visa, Residency Permit, BPSS report



- HMRC data to meet statutory reporting obligations such as; National Insurance Number, P45, Tax Code, UTR and/or VAT certification
- Personal Limited Company information to meet contractual and client framework agreements obligation, including; Certificate Of Incorporation, confirmation of Public Liability, Professional Indemnity and, where required Employer Liability cover, monitored for renewal
- Personal, Business and Proof of Engagement reference to support engagement history
- Security clearance documentation (monitored for annual renewal), SC to DV level clearance letters
- Employment records (including job titles, start date, work history, working hours, salary, payroll records, annual leave, pension and benefit information)
- Disciplinary and grievance information, including warnings issued to you
- Photographs
- Information about your use of our information and communications systems

Special categories of personal data

While we generally do not collect sensitive personal data, we may process specific Special Categories of Personal Data in the following limited circumstances where required by law:

- Health Information: We may collect information regarding sickness absence to calculate statutory sick pay and to ensure your health and safety in the workplace.
- Biometric Data: Biometric Data: We use a government-certified Identity Service Provider (IDSP) to verify your identity and Right to Work. This involves processing biometric data, such as comparing a selfie or video of you against the photo in your identity document. We do not retain the raw biometric data (such as the facial scan) ourselves; we only retain the report confirming the check was successful.
- Criminal Convictions: We may process information about criminal convictions where a high-level security clearance (SC to DV level) is a specific requirement of the client engagement.
- We may collect information about protected characteristics (such as ethnicity, disability, gender) for the purpose of monitoring equality of opportunity. Providing this information is voluntary and will not affect your employment or engagement. Data is used only for aggregated reporting and not for decision-making about individuals.

How is your personal information collected?

We collect personal information when you express an interest in working with us, as an employee, supplier or client. This may be directly via phone conversations, email, social media or our website, or sometimes through a recruitment agency or third party. We collect additional information from third parties including former employers, background check agencies, colleagues and professional networking websites such as LinkedIn. We will also collect additional personal information in the course of job-related activities from our own observations and records such as the services you provide or purchase, and our correspondence and relationship with you.

How we will use information about you

We only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Performance of Contract: Where we need to perform the contract we have entered into with you.
- Legal Obligation: Where we need to comply with a legal or regulatory obligation.
- Legitimate Interests: Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Vital Interests: Where we need to protect your vital interests (or someone else's interests).
- Consent: Where you have given us explicit consent to do so (for example, to use your photograph for marketing purposes). You may withdraw this consent at any time.



How we will process your information

Situations in which we will process your personal information include:

- Administering the contract we have entered into with you
- Assessing qualifications for a particular job or task
- To respond to your enquiries or queries.
- To improve the operation of the business and keep records of our interactions and communications with you
- Determining the terms on which you work for us
- Checking you are legally entitled to work in the UK
- Checking professional qualifications and security clearances
- To provide information to Clients about our employees
- Paying you, deducting tax, NI contributions and liaising with your pension provider if applicable
- Making decisions about continued employment or engagement
- Providing references to potential employers
- Using your photo for marketing purposes
- To otherwise conduct everyday business activities, such as business development, business planning, strategic reviews and statistical, evaluation and reporting purposes.

We will only use your personal information for the purposes for which it was collected, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Automated decision-making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you. We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

If you fail to provide personal data

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers) or we may be unable to discharge our legal or regulatory obligations.

Who has access to data?

We may need to share your data for the purposes set out above with the following parties:

- Identity Service Providers (IDSPs) who act as data processors to conduct digital Right to Work and identity verification checks on our behalf.
- Service providers based in the EEA who provide IT and system administration services.
- Professional advisers including HR consultants, lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance and accounting services.
- HM Revenue & Customs, regulators and other authorities.
- Third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy notice.

We require all third parties to respect the security of your personal data and to treat it in



accordance with the law. We do not allow our third party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions. We do not give anyone else access to your personal information in return for payment, for marketing or any commercial purposes.

International transfers

We may transfer your personal data to service providers, specifically Google and Microsoft, whose servers may be located outside the United Kingdom and the European Economic Area (EEA), including in the United States.

To ensure your data is protected to the same standard as it is in the UK, we rely on the following safeguards:

- Adequacy Regulations: Where data is transferred to the US, we rely on the UK Extension to the EU-US Data Privacy Framework, provided the recipient is certified under this framework (which both Google and Microsoft are).
- Standard Contractual Clauses (SCCs): In instances where an adequacy decision is not available, we ensure that specific contracts approved by the UK Information Commissioner's Office (International Data Transfer Agreements or IDTAs) are in place to give your personal data the same protection it has in the UK.

Further information about Google's privacy policies can be found at the following link:

<https://cloud.google.com/security/gdpr>

Further information about Microsoft's privacy policies can be found at the following link:

<https://privacy.microsoft.com/en-gb/privacystatement>

How do we protect data?

We take the security of your data seriously. We have internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties. Computers storing personal data are password and MFA protected and we have also invested in anti-malware software.

Where we engage third parties to process personal data on our behalf, they do so on the basis of written instructions, are under a duty of confidentiality, and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

For how long do we keep data?

We will only retain 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.

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.

Details of retention periods for different aspects of your personal data are available by contacting business.operations@swiftstrategies.co.uk

Here are key points for you to be aware of:

- We will keep your contact details for 7 years post our last meaningful contact or engagement with you. If we have not interacted with you or considered you for a project in this timeframe, we will securely delete your details from our contact database.
- We will keep other personal information for the duration of our trading relationship with you.



- In the course of our trading relationship with you, we will retain certain personal information, such as financial and tax information, orders and contracts, for at least 7 years following the completion, termination or expiry of the relevant order or contract with us. We may then destroy the information.

Your rights

Under data protection law, you have rights including:

- Your right of access - you have the right to ask us for copies of your personal information.
- Your right to rectification - you have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
- Your right to erasure - you have the right to ask us to erase your personal information in certain circumstances.
- Your right to restriction of processing - you have the right to ask us to restrict the processing of your personal information in certain circumstances.
- Your right to withdraw consent - where we rely on your consent (e.g. for photos), you have the right to withdraw this at any time.
- Your right to object to processing - you have the right to object to the processing of your personal information in certain circumstances.
- Your right to data portability - you have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you. If you would like to make a request, please contact business.operations@swiftstrategies.co.uk

How to complain

If you have any concerns about our use of your personal information, you can make a complaint to us by contacting Carolyn Venn at carolyn.venn@swiftstrategies.co.uk.

If you believe that we have not complied with your data protection rights, you can also complain to the Information Commissioner.

The ICO's address:

Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow
Cheshire, SK9 5AF

Helpline number: 0303 123 1113
ICO website: <https://ico.org.uk>

Notice review

Last updated January 2026
Next review January 2027

