Privacy Notice

SimIntel Ltd · Last updated: 01/11/2026

Summary

- We are SimIntel Ltd, a UK company providing solution architecture, cloud delivery and AI deployment services and developing the SimIntel AI Workbench product. We are the controller for the personal data described in this notice.
- When we work on a clients systems or data, the client is the controller and we act as its processor under our contract with the client (see section 2).
- We do not sell personal data and we do not allow the AI tools we use to train their models on your data.
- Most of our data is held in Microsoft 365 and Azure in the UK and Europe. Some of our providers are in the United States and we use legal safeguards for those transfers (section 8).
- You have rights over your personal data and can complain to us at privacy@simintel.co.uk or to the Information Commission.

1. Who we are and how to contact us

SimIntel Ltd ("SimIntel", "we", "us") is a company registered in England and Wales with company number **17472467**, whose registered office is at **5 Brayford Square, London, United Kingdom, E1 0SG**. We are registered with the Information Commission as a data controller, registration number **ZC280486.**

This notice explains how we collect, use, share and protect personal data when you:

- visit our website at www.simintel.co.uk ("Website");
- are a contact at a client, prospective client, partner or supplier, or otherwise communicate or do business with us;
- apply to work with us or work with us as a subcontractor or director (section 4).

We process personal data under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations (PECR), each as amended by the Data (Use and Access) Act 2025.

Contact. Email privacy@simintel.co.uk, with "Data Protection Request" in the subject line or write to us at the registered office address above. Our privacy lead is Chris Sharples, Director. We are not required to appoint a Data Protection Officer and have not done so.

2. Controller and processor roles

As a controller. We decide how and why personal data is used when we run our website, market our services, manage client and supplier relationships, engage people to work with us and run our business. This notice covers that processing.

As a processor. When we design, build or configure systems for a client, we may have access to personal data the client controls, for example in the clients Microsoft 365 or Azure tenant, in a dedicated Azure environment we run for the engagement or in a deployment of the SimIntel AI Workbench. We use that data only on the clients documented instructions, under a data processing agreement or the data protection terms of our contract. The SimIntel AI Workbench is deployed into the clients own environment and the client is the controller of the documents and data it processes.

If your personal data is held by one of our clients and you want to exercise your rights, please contact that client directly. If you contact us, we will pass your request to the client within 2 business days, tell you who the controller is and help the client respond.

3. Personal data we collect

Category	Examples	Source
Contact and relationship data	Name, job title, employer, business email address, telephone number, notes of our dealings with you	You, your organisation, publicly available business sources such as LinkedIn and company websites
Communications data	Emails, Teams messages and meeting content, including recordings, transcripts and AI generated meeting summaries where you have been told they are in use	You, when you communicate with us
Contract and billing data	Billing contact, purchase orders, invoices, payment records	You, your organisation
Engagement access data	Guest account identifiers and sign in records when you or we are given access to each other's systems	You, your organisation's identity provider, Microsoft Entra ID
Website and technical data	IP address, browser and device type, pages viewed, referring site.	Automatically, via cookies and similar technologies (section 9)
Marketing data	Marketing preferences, event attendance, responses to our messages	You
Complaints and rights requests	The content of your complaint or request and our correspondence about it	You or someone acting for you

Special category and criminal offence data. We do not seek special category data (such as health, ethnicity or religious beliefs) about client, supplier or website contacts. For people who work with us, see section 4. If you tell us about a health condition so that we can make adjustments, we use it only for that purpose.

Children. Our services are for businesses and are not directed at children. We do not knowingly collect personal data from anyone under 18.

4. Candidates, subcontractors and directors

If you apply to work with us or work with us as a subcontractor or director, we also process:

- Identity and right to work documents, CVs, employment or engagement history, references and evidence of qualifications;
- A basic criminal record check (Basic DBS) or client specific vetting, only where a client contract requires it, with your knowledge and under a condition in Schedule 1 of the Data Protection Act 2018;
- Contract, fee or payment details, bank details and tax information;
- Records of system access, company devices, training, and policy acknowledgements, kept to protect the information we and our clients entrust to us.

We use this data to decide whether to engage you, to meet our legal obligations (including right to work checks), to manage the engagement and to keep our and our clients information secure. Screening records are restricted to the directors.

5. How we use personal data and our lawful bases

Purpose	Lawful basis
Providing and delivering our services, including contract review, project delivery and support	Contract, where you are the client; otherwise legitimate interests in running our engagements with your organisation
Managing client, partner and supplier relationships, invoicing and payments	Contract; legal obligation for accounting and tax records

Purpose	Lawful basis
Securing our systems and our clients' information, including access control, sign-in monitoring, logging and incident response	Legitimate interests in keeping systems and information secure; legal obligation where we must report incidents
Engaging candidates, subcontractors and directors, including screening	Contract; legal obligation (right to work); legitimate interests in checking suitability; for criminal record checks, the Schedule 1 condition noted in section 4
Sending marketing to business contacts	Legitimate interests or consent where PECR requires it. You can opt out at any time
Running and improving our website	Legitimate interests; consent for non essential cookies
Handling complaints and data protection requests	Legal obligation
Meeting legal and regulatory obligations, establishing or defending legal claims, and certification audits of our management system	Legal obligation; legitimate interests

Where we rely on legitimate interests, we have balanced our interests against your rights. You can ask us for details. Where we rely on consent, you can withdraw it at any time without affecting processing before you withdrew it.

6. Artificial intelligence

We use AI tools in our own work, including Microsoft 365 Copilot, GitHub Copilot and Claude (Anthropic) under business licences. Before we use any AI tool, we complete an impact assessment covering the data it may process.

- Our business licences do not allow the providers to train their models on our inputs or outputs.
- Client personal data is used with AI tools only where our contract with the client allows it.
- AI output is reviewed by a person before we rely on it.

Automated decisions. We do not make decisions about you based solely on automated processing that have legal or similarly significant effects. If that changes, we will update this notice and give you the safeguards the law requires, including the right to human review.

7. Sharing personal data

We share personal data only as follows:

- Service providers that process data for us under contract, including Microsoft (Microsoft 365, Azure, Azure DevOps), GitHub, Anthropic and our accounting provider;
- Subcontractors working on an engagement, under contracts that include confidentiality and data protection terms;
- Professional advisers, insurers, banks and our certification body, where needed;
- Regulators, law enforcement and courts, where the law requires it or to establish or defend legal claims;
- A buyer or investor in connection with a sale, merger or reorganisation of our business, under confidentiality terms.

We do not sell personal data.

8. International transfers

We store most data in Microsoft 365 and Azure in UK and European data centres. Some providers process data in the United States, including GitHub and Anthropic. Where personal data leaves the UK, we use one of these safeguards:

- a country the UK recognises as providing adequate protection;

- the UK Extension to the EU-US Data Privacy Framework, where the US recipient is certified; or
- the UK International Data Transfer Agreement, or the EU Standard Contractual Clauses with the UK Addendum.

You can ask us for a copy of the relevant safeguard at privacy@simintel.co.uk.

9. Cookies

Our Website uses strictly necessary cookies to work. We set other cookies, such as analytics, only with your consent through our cookie banner or where PECR exempts them, for example certain analytics cookies used only to improve the website, in which case we tell you and let you object. You can change your choices at any time from the banner or your browser settings.

10. How long we keep personal data

Data	Retention
Client, partner and supplier contacts and correspondence	At least 1 year, then reviewed annually and deleted when no longer needed
Contracts, including NDAs and data processing agreements	6 years after the contract ends
Accounting, tax and invoicing records	6 years from the end of the financial year
Right-to-work records	2 years after the engagement ends
Unsuccessful candidates	3 months after the decision
Criminal record and vetting results	Only as long as the engagement that required them
Complaints, rights requests and security incident records	6 years
Marketing preferences	Until you opt out; we keep a suppression record so that we do not contact you again
Client data we process as a processor	As set by the client contract; by default, client environments are decommissioned at the end of the engagement and AI inferencing logs are deleted after 90 days

Where data is held in Microsoft 365 under a retention policy and you ask us to erase it, we put it beyond use until the retention period ends and then delete it.

11. Your rights

You have the right to:

- **be informed** about how we use your data (this notice);
- **access** a copy of your personal data;
- **rectification** of inaccurate or incomplete data;
- **erasure** in certain circumstances;
- **restrict** how we use your data in certain circumstances;
- **data portability** for data you gave us, where processing is based on consent or contract and is automated;
- **object** to processing based on legitimate interests, and to direct marketing at any time;
- **withdraw consent** where we rely on it.

To use your rights, email privacy@simintel.co.uk with "Data Protection Request" in the subject line. We will respond within one month, or up to three months for complex requests, in which case we will tell you within the first month. We may need to confirm your identity. For access requests, we carry out reasonable and proportionate searches. There is normally no fee.

12. Complaints

If you are unhappy with how we have handled your personal data, please complain to us first at privacy@simintel.co.uk or by any other means of contacting us. We will acknowledge your complaint within 30 days (we aim for 5 business days), investigate it, keep you informed and tell you the outcome in writing.

You also have the right to complain to the UK regulator, the Information Commission, at any time:

Information Commission

Website: ico.org.uk · Helpline: 0303 123 1113 · Post: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

13. Security

We operate an information security and quality management system aligned to ISO/IEC 27001:2022 and ISO 9001:2026. Our measures include:

- Company managed devices with disk encryption and Microsoft Defender;
- A single identity system (Microsoft Entra ID) with multi-factor authentication for every account, phishing-resistant authentication and just in time activation for administrative access;
- Encryption of data in transit and at rest, and least-privilege access on a need to know basis;
- A separate Azure environment for each client engagement;
- Logging, monitoring, backups, secure development practices and independent penetration testing of our product.

If a personal data breach is likely to put your rights at risk, we will report it to the Information Commission within 72 hours of becoming aware of it and tell you without undue delay if the risk to you is high. Where we act as a processor, we will tell the client without undue delay, as our contract requires.

14. Changes to this notice

We review this notice at least once a year and when our processing changes. We will publish any update on our Website with a new "Last updated" date and, where a change materially affects you, tell you directly.