

Evy-AI Workforce

Privacy Policy

Effective Date: July 2025 · Version 1.0

Saelle Group FZE LLC · Amber Gem Tower, Sheikh Khalifa Street, Dubai/Ajman, UAE

1. Introduction

Saelle Group FZE LLC, trading as Evy-AI Workforce (Evy-AI, we, us, or our), is committed to protecting the privacy and security of all personal data we handle — whether from visitors to our website, prospects engaging with our services, or individuals whose data is processed through our platform on behalf of our clients.

This Privacy Policy explains what personal data we collect, why we collect it, how we use and protect it, and what rights you have in relation to it. It applies to:

- Visitors and users of www.evy-ai.com and associated subdomains
- Prospects, leads, and clients who engage with Evy-AI Workforce services
- Data subjects whose personal information is processed through the Evy-AI platform on behalf of our clients ("End User Data")

This policy is governed by and compliant with the following regulatory frameworks:

- UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (PDPL)
 - Saudi Arabia's Personal Data Protection Law (PDPL-KSA)
 - UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018
 - EU General Data Protection Regulation (GDPR) — Regulation (EU) 2016/679
 - California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
 - US Health Insurance Portability and Accountability Act (HIPAA) — where applicable
-

2. Data Controller

The data controller responsible for your personal data is:

Saelle Group FZE LLC

Trading as: Evy-AI Workforce

Registered address: Amber Gem Tower, Sheikh Khalifa Street, Dubai/Ajman, UAE

Email: hello@evy-ai.com

Phone/WhatsApp: +971 52 244 5061

Website: www.evy-ai.com

Where Evy-AI processes personal data on behalf of a client (e.g. through an AI agent deployment), the client acts as the data controller and Evy-AI acts as the data processor. In such cases, a Data Processing Agreement (DPA) governs that relationship.

3. What Personal Data We Collect

3.1 Website Visitors

When you visit our website, we may collect:

- IP address, browser type, device type, and operating system
- Pages visited, time spent on pages, and referring URLs
- Cookie identifiers and analytics data (see Section 9 on Cookies)
- Any information you voluntarily submit via forms, including name, email, company name, phone number, and website

3.2 Prospects and Clients

When you engage with Evy-AI as a prospect or client, we collect:

- Contact details: first name, last name, email address, phone number
- Company details: company name, website, industry, and size
- Audit and assessment data: responses submitted through our AI Readiness Audit tool, including department selections, workflow answers, and readiness scores
- Communication records: emails, call recordings (where consented), and meeting notes
- Commercial data: contract details, invoicing information, and payment records

3.3 End User Data (Processed on Behalf of Clients)

Where Evy-AI deploys AI agents on behalf of a client, we may process personal data belonging to that client's customers, employees, or other end users. This may include:

- Names, contact details, and account information
- Interaction data: call recordings, chat transcripts, email content, and voice messages
- Document data: invoices, identification documents, and supporting materials submitted during interactions
- Behavioural data: interaction patterns, satisfaction signals, and escalation records

Evy-AI processes End User Data solely on the documented instructions of the client. We never use End User Data for our own purposes, marketing, or model training without explicit consent from the data controller.

4. How We Collect Personal Data

We collect personal data through the following means:

- Directly from you: when you complete our AI Readiness Audit, submit a contact form, book a strategy call, or communicate with us by email, phone, or WhatsApp
- Automatically: through cookies and analytics tools when you visit our website (see Section 9)
- From our clients: when a client engages our platform to process interactions on their behalf, personal data of their end users may be transmitted to us
- Through triggered data flows: Evy-AI never pulls data from a client's CRM or ERP system. Data is only transmitted when the client's system creates a trigger event. This architecture ensures your infrastructure remains in control at all times.

5. Legal Basis for Processing

We process personal data on the following legal grounds, depending on the context:

- Contractual necessity: to fulfil our obligations under a client contract or to take steps prior to entering into one
- Legitimate interests: to operate and improve our platform, respond to enquiries, and conduct business development activities — where these interests are not overridden by your rights
- Consent: where you have given clear, specific consent — for example, when submitting the AI Readiness Audit or subscribing to communications
- Legal obligation: where processing is required to comply with applicable law, regulation, or court order
- Vital interests: in rare circumstances where processing is necessary to protect life

For End User Data processed on behalf of clients, the legal basis is determined by the client as data controller. Evy-AI processes such data under the authority of a Data Processing Agreement.

6. How We Use Your Personal Data

6.1 Website Visitors

- To analyse website performance and improve user experience
- To understand how visitors find and interact with our content
- To respond to enquiries submitted through our website

6.2 Prospects and Clients

- To deliver and manage our AI deployment services
- To process and respond to AI Readiness Audit submissions
- To contact you regarding your enquiry, strategy call, or deployment
- To send relevant communications about Evy-AI services where you have consented or where legitimate interest applies
- To manage invoicing, contracts, and commercial relationships
- To comply with legal and regulatory obligations

6.3 End User Data

- To operate AI agents on behalf of clients — handling inbound and outbound interactions, processing requests, and executing workflows
 - To generate interaction summaries, quality scores, and coaching outputs for the benefit of the client
 - To improve interaction quality within the client's deployment — not across unrelated clients or for general model training
-

7. Data Architecture, Security and Compliance Certifications

7.1 Compliance Certifications

Evy-AI Workforce is certified to the following international security and compliance standards:

- ISO/IEC 27001 — Information Security Management
- SOC 2 Type II — Security, Availability, and Confidentiality
- GDPR — EU and UK General Data Protection Regulation
- HIPAA — Health Insurance Portability and Accountability Act
- PCI-DSS — Payment Card Industry Data Security Standard
- PDPL — UAE Personal Data Protection Law and KSA equivalent

7.2 In-Country Hosting

Every country in which Evy-AI operates is served by its own dedicated server infrastructure. Data is never transferred across borders without explicit authorisation. Your data stays in the jurisdiction where it was collected.

7.3 Two-Way Data Protection

Evy-AI does not pull data from your CRM, ERP, or any connected system. Data only flows when your system creates a trigger event — meaning your infrastructure initiates every data transfer. This two-way protection model is proprietary to Evy-AI and ensures your systems remain in control at all times.

7.4 Encryption and Access Controls

- End-to-end encryption in transit (TLS 1.2 minimum) and at rest (AES-256)
- Role-based access control (RBAC) limiting data access to authorised personnel only
- Multi-factor authentication (MFA) required for all system access
- Regular penetration testing and vulnerability assessments
- Full audit logs of all data access and processing events

7.5 On-Premise Deployment

For organisations requiring maximum data sovereignty, Evy-AI offers on-premise deployment using our proprietary Large Language Model. This configuration makes zero external API calls — your data never leaves your environment under any circumstances.

8. Data Retention

We retain personal data only for as long as necessary to fulfil the purposes described in this policy, or as required by law:

- Prospect and audit data: retained for 24 months from last contact, unless a contract is entered into
- Client and contract data: retained for 7 years from contract end to satisfy legal and financial obligations
- End User interaction data: retained according to the terms of the client Data Processing Agreement — typically 12–36 months unless otherwise specified
- Website analytics data: retained for 26 months (Google Analytics default), configurable on request
- Legal compliance records: retained as required by applicable law in each jurisdiction

On expiry of the applicable retention period, data is securely deleted or anonymised in a manner that prevents reconstruction.

9. Cookies and Analytics

Our website uses cookies and similar tracking technologies to understand how visitors use the site and to improve performance and user experience.

Types of cookies we use:

- Strictly necessary cookies: essential for the website to function. These cannot be disabled.
- Analytics cookies: we use Google Analytics (or similar tools) to collect anonymised data on page views, session duration, traffic sources, and user behaviour. This data does not personally identify you.
- Preference cookies: used to remember your settings and choices across sessions.

You can control cookies through your browser settings or by using our cookie consent tool when you first visit the site. Disabling analytics cookies will not affect your ability to use the website.

For more information on Google Analytics data practices, visit: policies.google.com/privacy

10. Who We Share Data With

We do not sell personal data. We do not share personal data with third parties for their own marketing purposes. We may share data in the following limited circumstances:

- Service providers: carefully selected third parties who provide infrastructure, analytics, CRM, or communication tools on our behalf — bound by confidentiality obligations and, where applicable, Data Processing Agreements
 - Clients: where End User Data is processed on behalf of a client, that data is accessible to the client as data controller
 - Legal authorities: where required by law, court order, or to protect the rights, safety, or property of Evy-AI, our clients, or the public
 - Business transfers: in the event of a merger, acquisition, or sale of assets, personal data may be transferred — subject to the same privacy protections described in this policy
-

11. International Data Transfers

Evy-AI's in-country hosting model means that data is stored and processed in the jurisdiction in which it is collected. Where any transfer of data across borders is required — for example, to a client or sub-processor in another country — we ensure that appropriate safeguards are in place, including:

- Standard Contractual Clauses (SCCs) approved by the European Commission or UK ICO
- Adequacy decisions where applicable
- Binding corporate rules or equivalent mechanisms

For UAE-based data, transfers comply with the requirements of the UAE PDPL. For UK data subjects, transfers comply with UK GDPR Article 46 mechanisms.

12. Your Data Rights

Depending on your jurisdiction, you may have the following rights in relation to your personal data:

All jurisdictions:

- Right to be informed: to know what data we hold and how we use it
- Right of access: to request a copy of the personal data we hold about you
- Right to rectification: to correct inaccurate or incomplete data
- Right to erasure: to request deletion of your data, subject to legal retention obligations
- Right to restrict processing: to limit how we use your data in certain circumstances
- Right to object: to object to processing based on legitimate interests or for direct marketing

UK and EU (GDPR) additional rights:

- Right to data portability: to receive your data in a structured, machine-readable format
- Rights related to automated decision-making and profiling

UAE (PDPL) rights:

- Right to access, correct, and request destruction of personal data

- Right to be informed of data breaches affecting your data

USA (CCPA/CPRA) rights:

- Right to know what personal information is collected, used, shared, or sold
- Right to opt out of the sale or sharing of personal information (we do not sell data)
- Right to non-discrimination for exercising your privacy rights
- Right to correct inaccurate personal information

To exercise any of these rights, contact us at hello@evy-ai.com. We will respond within 30 days (or sooner where required by applicable law). We may need to verify your identity before processing your request.

13. Data Breach Notification

In the event of a personal data breach that poses a risk to your rights and freedoms, Evy-AI will:

- Notify the relevant supervisory authority within 72 hours of becoming aware of the breach (where required by GDPR or equivalent law)
- Notify affected individuals without undue delay where the breach is likely to result in high risk to their rights
- Notify affected clients immediately where a breach involves End User Data processed on their behalf

All breach incidents are logged, investigated, and documented regardless of whether external notification is required.

14. Children's Privacy

Evy-AI Workforce services are directed exclusively at business customers and are not intended for individuals under the age of 18. We do not knowingly collect personal data from children. If you believe we have inadvertently collected data from a minor, please contact us immediately at hello@evy-ai.com and we will delete it promptly.

15. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, legal obligations, or operational requirements. When we make material changes, we will:

- Update the effective date at the top of this document
- Post the revised policy at www.evy-ai.com/privacy
- Notify active clients by email where the changes materially affect how we process their data

Your continued use of our website or services after the effective date constitutes acceptance of the updated policy.

16. Contact and Complaints

For any questions, requests, or concerns regarding this Privacy Policy or our data practices, please contact:

Evy-AI Workforce — Data Privacy

Saelle Group FZE LLC

Amber Gem Tower, Sheikh Khalifa Street, Dubai/Ajman, UAE

Email: hello@evy-ai.com

Phone / WhatsApp: +971 52 244 5061

Website: www.evy-ai.com

If you are located in the UK or EU and are not satisfied with our response, you have the right to lodge a complaint with your local supervisory authority:

- UK: Information Commissioner's Office (ICO) — ico.org.uk
- EU: Your national Data Protection Authority — edpb.europa.eu

If you are located in the UAE, you may contact the UAE Data Office — uaedataoffice.ae

If you are located in the USA, you may have the right to contact your state Attorney General or relevant consumer protection authority.

This Privacy Policy was last updated in July 2025. Version 1.0.

© 2025 Saelle Group FZE LLC trading as Evy-AI Workforce. All rights reserved.