Privacy Policy

Zysent Agency

Last Updated: August 12, 2025

---

1. Introduction

Zysent ("we," "us," or "our") is committed to protecting your privacy. This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you use our AI automation services, visit our website, or engage with our services.

2. Information We Collect

2.1 Personal Information

We may collect personal information that you voluntarily provide to us, including but not limited to:

- Name and contact information (email, phone, address)
- Company information and job title
- Payment and billing information
- Communications with us (emails, chat logs, support tickets)
- Account credentials and access tokens for third-party tools and platforms (collected only as necessary for AI automation implementation)
- Passwords and login information for software tools and platforms required for service delivery

2.2 Business Information

In the course of providing AI automation services, we may collect:

- Business data and processes you share with us
- System integration requirements and specifications
- Performance metrics and analytics data
- Technical information about your systems and workflows
- Configuration data necessary for ongoing service operation

2.3 Automatically Collected Information

We may automatically collect certain information, including:

- IP addresses and device identifiers
- Browser type and operating system
- Usage patterns and website interactions
- Cookies and similar tracking technologies

2.4 Third-Party Information

We may receive information from third-party sources, including:

- Business partners and referral sources
- Public databases and social media platforms
- Third-party service providers and integrations

3. How We Use Your Information

3.1 Service Delivery

We use your information to:

- Provide AI automation services and support
- Develop and implement custom AI workflows
- Monitor and maintain AI systems performance
- Process payments and manage billing

3.2 Communication

We use your information to:

- Respond to inquiries and provide customer support
- Send service updates and technical notifications
- Share relevant industry insights and updates
- Conduct surveys and gather feedback

3.3 Business Operations

We use your information to:

- Improve our services and develop new features
- Conduct research and analytics
- Comply with legal obligations
- Protect against fraud and security threats

4. Information Sharing and Disclosure

4.1 Third-Party Service Providers

We may share information with various third-party service providers who assist us in delivering AI automation services. These providers vary depending on the specific solution being implemented and may include:

- Cloud computing and data storage platforms
- Payment processing and billing services
- Analytics and performance monitoring tools
- Customer support and communication platforms
- AI and automation platforms and APIs
- Integration tools and middleware services

The specific third-party services used will be determined by the requirements of your AI automation solution and will be disclosed as part of the project implementation process.

4.2 Business Transfers

In the event of a merger, acquisition, or sale of assets, your information may be transferred to the acquiring entity.

4.3 Legal Requirements

We may disclose information when required by law, court order, or government request, or to protect our rights and safety.

4.4 Consent-Based Sharing

We may share information with your explicit consent for specific purposes.

5. Data Security

5.1 Security Measures

We implement appropriate technical and organizational security measures to protect your information, including:

- Encryption of data in transit and at rest
- Access controls and authentication systems
- Secure handling and storage of credentials and sensitive data
- Regular security assessments and monitoring
- Employee training on data protection
- Immediate deletion of sensitive credentials upon project completion when possible

5.2 Credential Management

For account credentials, passwords, and access tokens required for AI automation implementation:

- We collect only the minimum credentials and passwords necessary for service delivery
- Sensitive credentials and passwords are typically not retained after project completion
- When ongoing access is required for service functionality, credentials and passwords are stored using industry-standard security practices including encryption and secure password management systems
- We implement role-based access controls to limit credential access to authorized personnel only
- All password handling follows security best practices including secure transmission and storage protocols

5.2 Data Breach Response

In the event of a data breach, we will notify affected individuals and relevant authorities as required by applicable law.

6. Data Retention

6.1 Retention Periods

We retain your information for as long as necessary to:

- Provide ongoing AI automation services
- Comply with legal obligations
- Resolve disputes and enforce agreements
- Pursue legitimate business interests

Sensitive credentials and passwords are typically deleted immediately upon project completion, unless ongoing access is required for service functionality. Configuration data and technical information necessary for service operation may be retained for the duration of the service relationship.

6.2 Data Deletion

Upon request or when no longer needed, we will securely delete or anonymize your personal information, subject to legal and technical constraints. For ongoing services, certain technical data may need to be retained to ensure proper system functionality.

7. Your Rights and Choices

7.1 Access and Correction

You have the right to access, update, or correct your personal information.

7.2 Data Portability

You may request a copy of your personal information in a structured, machine-readable format.

7.3 Deletion Rights

You may request deletion of your personal information, subject to legal and contractual limitations.

7.4 Opt-Out Rights

You may opt out of certain communications and data processing activities.

7.5 Complaint Rights

You have the right to file complaints with relevant data protection authorities.

8. Cookies and Tracking Technologies

8.1 Cookie Usage

We use cookies and similar technologies to:

- Enhance website functionality and user experience
- Analyze website usage and performance
- Provide personalized content and services
- Support security and fraud prevention

8.2 Cookie Management

You can manage cookie preferences through your browser settings or our cookie management tools.

9. International Data Transfers

9.1 Global Operations

As we provide services internationally, your information may be transferred to and processed in countries other than your residence.

9.2 Transfer Safeguards

We implement appropriate safeguards to ensure adequate protection of transferred data, including standard contractual clauses and adequacy determinations.

10. Children's Privacy

Our services are not directed to individuals under the age of 16, and we do not knowingly collect personal information from children under 16. If we become aware of such collection, we will delete the information promptly.

11. California Privacy Rights

11.1 CCPA Rights

California residents have specific rights under the California Consumer Privacy Act, including rights to know, delete, and opt-out of the sale of personal information.

11.2 Do Not Sell

We do not sell personal information as defined by the CCPA.

12. Regional Compliance and Industry Regulations

12.1 GDPR Compliance

We comply with the General Data Protection Regulation (GDPR) for EU residents, including providing lawful bases for processing and respecting individual rights. For AI automation services delivered to EU clients, we ensure that all third-party integrations and data processing activities meet GDPR requirements.

12.2 HIPAA Compliance

When providing AI automation services that involve protected health information (PHI), we implement additional safeguards to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA), including:

- Execution of Business Associate Agreements (BAAs) when required
- Implementation of administrative, physical, and technical safeguards
- Ensuring all third-party integrations are HIPAA-compliant when handling PHI

12.3 Industry-Specific Regulations

Depending on your industry and the nature of the AI automation services provided, we may need to comply with additional regulations such as:

- Financial services regulations (PCI DSS, SOX, etc.)
- Healthcare regulations beyond HIPAA
- Government and public sector compliance requirements
- International data protection laws and frameworks

12.4 Legal Bases

Our legal bases for processing include consent, contract performance, legitimate interests, and legal compliance. Specific legal bases will be identified based on the nature of the AI automation services and applicable regulatory requirements.

13. Updates to This Privacy Policy

We may update this Privacy Policy from time to time. Material changes will be communicated through email or website notices. Your continued use of our services constitutes acceptance of the updated policy.

14. Contact Information

For questions about this Privacy Policy or to exercise your privacy rights, please contact us:

Zysent
Saida, Algeria
support@zysent.com
+213 (56) 299-4712

We do not currently have a designated Data Protection Officer, but privacy inquiries can be directed to the above contact information.

This Privacy Policy is effective as of the date listed above and applies to all information collected by Zysent.