

Unicon Group Ltd.

PRIVACY POLICY

Effective Date: May 1, 2026

Last Updated: June 10, 2026

1. Introduction

This Privacy Policy describes how Unicon Group Ltd., ("Unicon," "we," "us," or "our") collects, uses, discloses, and safeguards information in connection with our business-to-business (B2B) software products, professional support services, and training programs (collectively, the "Services").

This Policy applies to our corporate website (the "Site") and all business interactions with our clients, prospects, and partners. We are committed to protecting the confidentiality of business information and complying with applicable privacy laws and regulations.

By accessing our Site or engaging with our Services, you acknowledge that you have read and understood this Privacy Policy.

2. Scope and Applicability

This Privacy Policy applies to:

- Organizations and business entities that purchase or evaluate our software, support, or training services
- Authorized representatives, employees, and agents of client organizations who interact with us on behalf of their organization
- Visitors to our corporate website
- Individuals who contact us for business inquiries, sales discussions, or support requests

This Policy does not apply to the internal data processing practices of our clients, which are governed by separate data processing agreements where applicable.

3. Information We Collect

3.1 Business Contact Information

In the course of our business relationships, we may collect:

- Business name, address, and contact details
- Names and professional titles of authorized contacts and account representatives
- Business email addresses and telephone numbers
- Job function and department information
- Company size, industry, and relevant business profile information

3.2 Transaction and Account Information

To fulfill contractual obligations and manage client accounts, we collect:

- Software licensing and subscription details
- Support ticket history, service requests, and case records
- Training enrollment records and completion status
- Executed contracts, agreements, statements of work, and related documentation
- ACH banking information and business check details provided for payment processing
- Invoice and billing records

3.3 Technical and Usage Information

In connection with the delivery and support of our software products, we may collect:

- Software version and configuration data necessary to provide support
- Error logs and diagnostic information submitted as part of support requests
- System environment information relevant to software deployment

3.4 Communications

We retain records of business communications including:

- Emails, written correspondence, and support communications
- Notes and records from sales, implementation, and support interactions
- Feedback, survey responses, and product inquiries

4. Website Visits and Cookies

We do not collect cookies, tracking technologies, or persistent identifiers from visitors to our corporate website. Specifically:

- No cookies are placed on your device when you visit our Site
- No analytics or behavioral tracking tools are deployed on our Site
- No third-party advertising or retargeting technologies are used
- No session tracking or cross-site tracking occurs

As a result, we do not collect IP addresses, browser fingerprints, device identifiers, or behavioral data from general website visitors. We are committed to maintaining a privacy-respecting web presence for our business clients and prospects.

5. Payment Processing

We accept payment exclusively through the following business payment methods:

- ACH (Automated Clearing House) electronic transfers
- Business checks

We do not accept credit cards, debit cards, or any consumer payment instruments for any of our products or services, including software licenses, support agreements, or training programs. This applies without exception.

ACH banking information provided for payment purposes is used solely to process authorized transactions and is handled in accordance with NACHA Operating Rules and applicable banking regulations. This information is

retained only as required for accounting, audit, and regulatory compliance purposes and is never sold or shared with unauthorized third parties.

6. How We Use Information

We use the information we collect for the following legitimate business purposes:

- Executing and managing software licensing agreements, support contracts, and training engagements
- Processing and reconciling ACH and business check payments
- Providing technical support, maintenance, and professional services
- Delivering training programs and issuing completion records
- Managing client accounts, renewals, and ongoing business relationships
- Communicating regarding product updates, security patches, and service notifications
- Complying with legal obligations, including tax and financial reporting requirements
- Enforcing our contractual rights and resolving disputes
- Improving our products and services based on client feedback

7. Disclosure of Information

7.1 No Sale of Information

We do not sell, rent, or trade business contact information or client data to any third party under any circumstances.

7.2 Service Providers

We may share information with trusted third-party service providers who assist us in operating our business, including cloud infrastructure providers, accounting and financial services firms, legal counsel, and IT service providers. All such providers are contractually required to maintain confidentiality and use information only for the specified business purpose.

7.3 Legal Requirements

We may disclose information when required by applicable law, regulation, court order, or governmental authority, or when necessary to protect our legal rights, prevent fraud, or ensure the safety of persons or property.

7.4 Business Transfers

In the event of a merger, acquisition, sale of assets, or similar corporate transaction, client information may be transferred as part of that transaction. We will provide notice of any such change and any applicable choices where required by law.

8. Data Retention

We retain business information for as long as necessary to fulfill the purposes described in this Policy, maintain an active client relationship, and comply with our legal and contractual obligations. Retention periods are guided by:

- The duration of the contractual relationship plus applicable post-termination periods
- Statutory requirements for financial and tax records (generally seven years)
- Applicable statutes of limitation for legal claims
- Our legitimate interest in maintaining records for dispute resolution

When information is no longer required for these purposes, we dispose of it securely.

9. Data Security

We implement and maintain commercially reasonable administrative, technical, and physical safeguards to protect business information against unauthorized access, disclosure, alteration, and destruction. Our security practices include:

- Access controls limiting data access to authorized personnel with a legitimate business need
- Encryption of sensitive data in transit and at rest where appropriate
- Regular review of information security policies and procedures
- Vendor due diligence for third-party service providers who access client information

While we take these measures seriously, no security system is impenetrable. In the event of a data security incident that affects your organization, we will notify you in accordance with applicable law and our contractual obligations.

10. Your Rights and Choices

Authorized representatives of client organizations may contact us to:

- Review or correct business contact information we maintain on file
- Request information about the categories of data we hold related to your organization
- Request deletion of business contact information where we have no ongoing legal or contractual obligation to retain it
- Update communication preferences for marketing and non-essential communications

Requests may be submitted to the contact information provided in Section 13. We will respond to verified requests within a reasonable timeframe and in accordance with applicable law. Note that certain information may be retained as required by law or necessary to fulfill our contractual obligations.

11. Third-Party Links and Services

Our website may contain links to third-party websites for informational purposes. We are not responsible for the privacy practices of those websites, and this Policy does not apply to them. We encourage you to review the privacy policies of any third-party sites you visit.

12. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, legal requirements, or business operations. The "Last Updated" date at the top of this document indicates when the most recent revision was made.

For material changes, we will provide notice to active clients through our standard communication channels. Continued use of our Services following notice of a material change constitutes acceptance of the updated Policy.

13. Contact Information

For questions, concerns, or requests related to this Privacy Policy, please contact us at: **Unicon Group Ltd.**
1748 Gilsinn Lane St. Louis, MO 63026 Email: support@unicongl.com Phone: 636.394.2012