DATA PROTECTION POLICY

Effective Date: January 1, 2025

1. INTRODUCTION

This Data Protection Policy ("Policy") describes how Palex Group ("we," "our," or "us"), operating through e-verifika.com and beta.e-verifika.com (collectively, the "Service"), protects and processes data in connection with Verifika, our SaaS translation quality control service. This Policy is intended for current and prospective clients and demonstrates our commitment to data security, privacy, and compliance with applicable data protection regulations.

Verifika is designed to provide translation quality assurance services while maintaining the highest standards of data protection. We implement technical and organizational measures to ensure the confidentiality, integrity, and availability of client data.

2. SCOPE AND APPLICATION

This Policy applies to all data processed through the Verifika Service, including:

- Client account information and authentication credentials
- Translation files and documents uploaded for quality control
- Quality control reports and analysis results
- Usage logs and technical metadata
- Payment and billing information (processed by our payment partner)

3. DATA CONTROLLER INFORMATION

Data Controller: Palex Group

Website: palexgroup.com

Service URLs: beta.e-verifika.com

Jurisdiction: United States

4. INFRASTRUCTURE AND TECHNICAL SECURITY

4.1 Hosting and Infrastructure

Verifika is hosted on Microsoft Azure cloud infrastructure with the following specifications:

- Hosting Provider: Microsoft Azure
- Data Center Location: West Europe region
- Infrastructure: Virtual machines managed by Kubernetes orchestration
- Database: Azure Database for PostgreSQL Flexible Server 16
- Real-time Communications: Microsoft SignalR Service

Microsoft Azure maintains certifications including SOC 1, SOC 2, SOC 3, ISO 27001, ISO 27018, HIPAA, FedRAMP, and other compliance standards. The West Europe data center provides enterprise-grade physical security, environmental controls, and redundant systems.

4.2 Application Architecture

Verifika employs a modern, security-focused architecture:

- Backend: .NET 8 framework with microservices architecture
- Frontend: Angular 18 with secure client-side processing
- Authentication: Dedicated OAuth 2.0 authorization server
- Database Security: Row-Level Security (RLS) implementation with UUID identifiers
- Architecture Pattern: Service-oriented architecture with isolated components

4.3 Data Isolation and Multi-Tenancy

We implement strict data isolation measures to ensure client data remains segregated:

- Row-Level Security (RLS) enforced at the database layer ensures clients can only access their own data
- Universally Unique Identifiers (UUIDs) prevent enumeration attacks and data leakage
- Application-level authorization checks validate access permissions for every request
- Kubernetes namespace isolation separates service components

5. DATA SECURITY MEASURES

5.1 Encryption

- Data in Transit: All data transmitted to and from the Service is encrypted using TLS 1.2 or higher with strong cipher suites
- Authentication Tokens: OAuth 2.0 tokens are securely generated, transmitted, and stored with industry-standard encryption

5.2 Access Controls

- Authentication: OAuth 2.0 protocol with secure token management
- Authorization: Role-based access control (RBAC) with principle of least privilege
- Administrative Access: Multi-factor authentication (MFA) required for all administrative functions
- Session Management: Secure session handling with automatic timeout and token rotation

5.3 Network Security

- Firewall Protection: Azure-managed firewalls with restrictive inbound rules
- DDoS Protection: Azure DDoS Protection Standard for infrastructure resilience
- Network Segmentation: Isolated virtual networks for different service components
- Intrusion Detection: Continuous monitoring for suspicious network activity

5.4 Application Security

- Secure Development: Security-focused coding practices and regular code reviews
- Input Validation: Comprehensive validation and sanitization of all user inputs

- Dependency Management: Regular updates and vulnerability scanning of third-party components

6. DATA PROCESSING PRINCIPLES

We adhere to the following data processing principles:

- Purpose Limitation: Data is processed solely for providing translation quality control services
- Data Minimization: We collect and process only data necessary for service delivery
- Accuracy: We maintain reasonable measures to ensure data accuracy and currency
- Storage Limitation: Data is retained only as long as necessary for service provision or as required by law
- Integrity and Confidentiality: We implement appropriate security measures to protect data

7. DATA CATEGORIES AND PROCESSING ACTIVITIES

7.1 Account Data

Data Types: email address, company information, account credentials

Purpose: User authentication, account management, service provision, and communication

Retention: Duration of account plus 90 days, or as required by law

7.2 Content Data

Data Types: Translation files, quality control reports, analysis results

Purpose: Providing translation quality assurance services

Retention: As determined by client; clients can delete content at any time

7.3 Usage Data

Data Types: Access logs, feature usage statistics, performance metrics, error logs

Purpose: Service optimization, troubleshooting, security monitoring, and service improvement

Retention: 90 days for operational logs; aggregated anonymized metrics retained indefinitely

7.4 Payment Data

Payment processing is handled entirely by our e-commerce partner, PayPro Global Inc. (payproglobal.com). We do not collect, process, or store payment card information. PayPro Global Inc. is PCI-DSS compliant and handles all payment transactions securely. We receive only transaction confirmation and basic billing information necessary for account management.

8. THIRD-PARTY SERVICE PROVIDERS

We engage the following third-party service providers who may process client data:

8.1 Microsoft Azure

Service: Cloud infrastructure and hosting

Purpose: Data storage, processing, and service hosting

Location: West Europe data center

Compliance: SOC 1/2/3, ISO 27001, ISO 27018, GDPR-compliant data processing

8.2 PayProGlobal

Service: Payment processing and e-commerce services

Purpose: Processing subscription payments and billing

Data Shared: Account identifier, subscription information (no payment card data shared with us)

Compliance: PCI-DSS compliant

All third-party processors are required to maintain appropriate security measures and process data only in accordance with our instructions and applicable data protection laws.

9. DATA SUBJECT RIGHTS

We respect data subject rights and provide mechanisms to exercise these rights:

- Right of Access: Clients can access their data through their account
- Right to Erasure: Clients can request deletion of their account and associated data
- Right to Data Portability: Clients can export their content data
- Right to Object: Clients can object to certain processing activities

To exercise these rights, clients may use the Service interface or contact us through the channels provided in Section 15.

10. DATA BREACH NOTIFICATION

In the event of a data breach that affects client data, we will:

- Investigate and contain the breach immediately upon discovery
- Notify affected clients without undue delay, and where feasible, within 72 hours of becoming aware of the breach
- Provide information about the nature of the breach, affected data categories, and remedial measures taken
- Cooperate with clients in meeting their own notification obligations under applicable data protection laws
- Document the incident and implement measures to prevent similar breaches

11. BUSINESS CONTINUITY AND DISASTER RECOVERY

We maintain business continuity and disaster recovery procedures to ensure service availability and data protection:

- Automated Backups: Daily automated backups of all client data with geo-redundant storage
- Backup Retention: Backups retained for 30 days with point-in-time recovery capability
- High Availability: Kubernetes-orchestrated containers with automatic failover and load balancing
- Recovery Time Objective (RTO): Target service restoration within 4 hours
- Recovery Point Objective (RPO): Maximum data loss limited to 24 hours
- Regular Testing: Disaster recovery procedures tested quarterly

12. MONITORING AND AUDITING

We implement comprehensive monitoring and auditing practices:

- Security Monitoring: 24/7 automated monitoring for security threats and anomalies
- Access Logging: Comprehensive logging of system access and administrative actions
- Audit Trails: Tamper-evident audit logs for critical security events
- Regular Reviews: Periodic review of security logs and access patterns
- Compliance Audits: Regular internal audits of security controls and data protection measures

13. EMPLOYEE ACCESS AND TRAINING

13.1 Access Controls

- Least Privilege: Employees are granted access only to data necessary for their role
- Authentication: Multi-factor authentication required for all employee access
- Access Reviews: Regular review and recertification of employee access rights
- Termination Procedures: Immediate revocation of access upon employment termination

13.2 Training and Awareness

- Security Training: Mandatory security awareness training for all employees
- Data Protection: Specific training on data protection principles and obligations
- Incident Response: Training on security incident identification and reporting
- Confidentiality: All employees sign confidentiality agreements

14. INTERNATIONAL DATA TRANSFERS

Client data is stored and processed in the Microsoft Azure West Europe data center. For clients located outside the European Economic Area (EEA), we rely on appropriate safeguards for data transfers, including:

- Microsoft Azure's comprehensive data protection
- Technical and organizational measures that ensure an adequate level of data protection

Clients requiring data residency in specific jurisdictions should contact us to discuss custom deployment options.

15. CONTACT INFORMATION

For questions about this Policy, data protection practices, or to exercise data subject rights, please contact us:

Palex Group

Website: e-verifika.com, palexgroup.com

Service: beta.e-verifika.com

Email: support@e-verifika.com

We will respond to inquiries within 30 days of receipt.

16. POLICY UPDATES

We may update this Policy periodically to reflect changes in our practices, technologies, legal requirements, or other factors. Material changes will be communicated to clients through:

- Email notification to registered account holders
- Prominent notice on our website and Service interface
- Updated effective date at the top of this Policy

Continued use of the Service after Policy updates constitutes acceptance of the revised Policy. Clients who do not agree with changes may terminate their accounts in accordance with our Terms of Service.

17. COMPLIANCE AND CERTIFICATIONS

Verifika's data protection framework aligns with recognized international standards and best practices:

17.1 Standards Alignment

- General Data Protection Regulation (GDPR): Our practices support GDPR compliance for EU-based clients
- California Consumer Privacy Act (CCPA): We honor California residents' privacy rights
- ISO 27001: Our infrastructure provider maintains ISO 27001 certification
- SOC 2 Type II: Microsoft Azure's SOC 2 compliance extends to our infrastructure

18. ACKNOWLEDGMENT

This Data Protection Policy demonstrates Palex Group's commitment to protecting client data and maintaining the highest standards of data security and privacy. We continuously review and enhance our practices to address evolving threats and regulatory requirements.

By using Verifika, clients acknowledge that they have read, understood, and agree to the practices described in this Policy. We value the trust our clients place in us and remain dedicated to safeguarding their data.

Document Version: 1.1.25
Last Updated: January 2025