WIDGERA AI AGENT PRIVACY POLICY

Effective Date: *November* 26, 2025

1. WHO WE ARE

Widgera Inc. ("Widgera," "we," "us," "our") is a Delaware corporation that develops AI-powered chat assistants ("AI Agents") deployed by our business customers ("Clients") on their websites and communication channels. Our AI Agents provide customer service, analytics insights, and customer relationship management capabilities.

Contact Information:

- **Company:** Widgera Inc.
- **Address:** 1111B S Governors Ave #23248, Dover, Delaware 19904, United States
- **Email:** support@widgera.com
- **Website:** https://widgera.com

2. SCOPE AND APPLICATION

This Privacy Policy governs how Widgera AI Agents process personal information from end users ("End Users") who interact with AI Agents deployed by our Clients. This policy covers:

- Data processing through AI Agent conversations
- Analytics chat conversations and insights processing
- CRM data collection and storage
- Optional Customer Insights profiling feature
- Data storage and retention practices
- End User rights and choices

This policy does not cover:

- Widgera's corporate website (widgera.com)
- Other Widgera products and services
- Client's own data practices on their websites

3. DATA CONTROLLER AND PROCESSOR ROLES

3.1 Role Definitions

- **Client as Data Controller:** Our Clients act as data controllers for End User chat data, determining the purposes and legal basis for processing
- **Widgera as Data Processor:** We process End User data solely under Client instructions as outlined in our Data Processing Addendum (DPA)
- **Widgera as Controller:** We act as controller only for our own operational data and Client account management

3.2 Legal Basis

Processing is based on the legal basis chosen by the Client, which may include:

- Consent (where required by applicable law)
- Legitimate interests (with right to object)
- Contract performance
- Legal obligations

4. DEFAULT DATA PROCESSING (MINIMAL RETENTION)

By default, AI Agents operate with minimal data retention:

4.1 Transient Processing Only

- Chat content is processed in real-time to generate responses
- No chat content is retained beyond technical necessity (typically 24 hours)
- Only operational metadata is preserved for system functionality

4.2 Limited Analytics

We maintain minimal, de-identified analytics including:

- Conversation counts and session metrics
- System performance and error rates
- Usage statistics for reliability monitoring
- Security and abuse prevention data

5. ENHANCED FEATURES: CRM AND ANALYTICS

Clients may enable enhanced features for customer relationship management and analytics insights.

5.1 Customer Relationship Management (CRM)

Data Categories When CRM is Enabled:

Contact Information:

- Names, email addresses, and phone numbers voluntarily provided
- Communication preferences and contact history
- Business context and interaction summaries
- User-selected information for storage

Interaction Data:

- Conversation topics and preferences expressed by users
- Service history and interaction patterns
- Communication channel preferences
- Custom tags and categorization chosen by users

Metadata:

- Interaction timestamps and frequency
- Geographic location (city/region level from IP address)
- Device and browser information (basic)
- Session identifiers and context

5.2 Analytics Chat Processing

Enhanced Analytics Conversations:

Chat Content:

- Messages exchanged in analytics-focused conversations
- User questions about business data and insights
- AI responses and analysis provided
- Historical conversation context for service continuity

Business Insights Processing:

- Patterns and insights extracted from conversation content
- Analytics interpretations and recommendations
- Custom analysis requests and results
- Trend identification and reporting data

Conversation Context:

- Previous analytics discussions for continuity
- User preferences for analytics delivery
- Historical context for improved insights
- Personalized analytics recommendations

5.3 Purposes of Enhanced Processing

Customer Relationship Management:

- Maintaining customer contact information and preferences
- Tracking interaction history for service continuity
- Personalizing service delivery based on past interactions
- Supporting customer retention and satisfaction efforts

Analytics and Insights:

- Processing business data to generate insights and patterns
- Answering questions about analytics and trends
- Providing personalized analytics recommendations
- Creating custom reports and analysis

Service Quality Enhancement:

- Improving response relevance through conversation history
- Reducing repetitive explanations and questions
- Enabling advanced customer service capabilities
- Supporting data-driven business decisions

5.4 Data Retention for Enhanced Features

Registered Users:

- **CRM Data:** Up to 24 months (configurable by Client)
- **Analytics Chat History:** Up to 24 months for conversation continuity
- **Business Insights:** Retained according to Client settings
- **Contact Information:** Until deletion requested or account closure

Unregistered Users:

- **All Data:** Automatically deleted after 7 days
- **No Profiling:** No long-term behavioral analysis
- **Temporary Storage:** Cookie-based identification for service continuity only

- **Immediate Deletion:** Available upon request via chat interface

5.5 Strictly Prohibited Processing

We explicitly prohibit creation or use of:

Sensitive Inferences:

- Special categories of data (health, religion, political opinions, sexual orientation, racial/ethnic origin)
- Biometric categorization or emotion recognition
- Social scoring or trustworthiness evaluations
- Criminal propensity or legal compliance assessments

Discriminatory Processing:

- Any processing that could result in unfair treatment
- Automated decisions with legal or significant effects
- Processing that enables discrimination based on protected characteristics
- Social profiling for exclusionary purposes

5.6 Automated Decision-Making Limitations

- No legal or similarly significant decisions made solely through automated processing
- End Users can request human review of any automated assessments
- All automated processing assists rather than replaces human decision-makers
- Transparent explanation of automated processing logic available upon request

6. PRIVACY NOTICE AND CONSENT

6.1 Unregistered User Consent

Minimally Intrusive Notice:

- Small text notice below chat input for first 3 messages
- Format: "*By chatting, you agree to our privacy practices. [Privacy Policy]*"
- Clear opt-out options before CRM data storage
- No processing beyond basic chat functionality without consent

Consent Collection:

- Clear explanation before any CRM data storage
- Option to continue without data storage

- Easy withdrawal of consent at any time
- Granular consent for different processing purposes

6.2 Registered User Consent

Account-Based Consent:

- Comprehensive privacy notice during account creation
- Detailed explanation of CRM and analytics features
- Optional feature activation with clear consent
- Ongoing consent management through account settings

6.3 Consent Management

Withdrawal Options:

- Easy consent withdrawal through chat interface
- Account settings for registered users
- Customer service assistance available
- Immediate processing cessation upon withdrawal

7. END USER RIGHTS AND CHOICES

7.1 Universal Rights

Access and Control:

- **Data Access:** Information about stored data and processing purposes
- **Data Correction:** Update inaccurate information in CRM or profiles
- **Data Deletion:** Request removal of all stored data
- **Processing Restrictions:** Limit specific types of processing
- **Data Portability:** Receive data in machine-readable format

CRM and Analytics Rights:

- **CRM Opt-Out:** Stop storing data in CRM system
- **Analytics Limitation:** Restrict analytics processing
- **Conversation Export:** Download chat history and insights
- **Profile Access:** View any generated customer profiles

7.2 Regional Privacy Rights

European Union and United Kingdom (GDPR/UK GDPR):

- Right to object to processing, including profiling
- Right to human review of automated decision-making
- Right to lodge complaints with supervisory authorities
- Right to restrict processing for specific purposes
- Right to data portability in structured format

United States - California (CCPA/CPRA):

- Right to know about data collection and use
- Right to delete personal information
- Right to correct inaccurate information
- Right to opt-out of sale/sharing (we do not sell data)
- Right to non-discrimination for exercising rights

Other Jurisdictions:

- Similar rights extended worldwide per local privacy laws
- Proactive compliance with emerging privacy regulations
- Accommodation of specific regional requirements

7.3 Exercising Rights

Unregistered Users:

- **In-Chat Requests:** Type deletion or opt-out requests directly in chat
- **Immediate Response:** Requests processed within 24-48 hours
- **Automatic Deletion:** All data removed after 7 days automatically
- **Support Assistance:** Email support@widgera.com for complex requests

Registered Users:

- **Account Dashboard:** Self-service options for most rights
- **Email Requests:** support@widgera.com with "Privacy Rights Request"
- **Customer Service:** Assistance through multiple channels
- **Client Channels:** Exercise rights through Client's customer service

Verification Process:

- Identity verification for security purposes
- Account verification for account-related requests
- Minimal information required for verification
- Alternative verification methods for unregistered users

8. DATA SHARING AND SUB-PROCESSORS

8.1 Authorized Sub-Processors

AI and Analytics Services:

- **OpenAI:** For natural language processing and conversation generation
- **Google AI/Gemini:** For advanced analytics and insights processing
- **Machine Learning Services:** For pattern recognition and analytics

Infrastructure Services:

- **Google Cloud Platform:** For hosting, storage, and computing (region-specific)
- **Database Services:** For secure data storage and retrieval
- **Content Delivery Networks:** For performance optimization

Support Services:

- **Monitoring Tools:** For performance and security monitoring
- **Analytics Platforms:** For usage analytics and optimization
- **Communication Services:** For customer notifications and support

8.2 Geographic Processing

Region-Specific Data Handling:

- **European and Regional Data:** For users in the **European Union, UK, Switzerland, and Georgia**, data is processed and stored exclusively within the **European Union**.
- **US and Global Data:** Processed and stored within the United States.
- **No Cross-Border Transfers:** We do not transfer data belonging to European or Georgian users to the United States without appropriate legal safeguards (such as SCCs).

8.3 Client Data Sharing

Authorized Sharing:

- Clients receive access to their own CRM data and analytics
- Aggregated insights from their customer interactions only
- Performance metrics for their AI agents
- Compliance and audit reports as requested

Data Isolation:

- Strict separation between different Client data
- No cross-Client data sharing or analysis
- Independent processing environments
- Isolated analytics and CRM databases

8.4 Sub-Processor Management

Current Sub-Processor List: https://widgera.com/legal/subprocessors

Change Management:

- 30-day advance notice for material changes
- Right to object to new sub-processors
- Alternative arrangements for objections
- Regular security assessments and audits

9. INTERNATIONAL DATA TRANSFERS

9.1 Transfer Mechanisms

EU/UK Transfers:

- **Standard Contractual Clauses (SCCs)** with UK Addendum
- **Adequacy Decisions** where available
- **Transfer Impact Assessments** conducted and available upon request

Other International Transfers:

- **Appropriate Safeguards** as required by applicable law
- **Contractual Protection** in all service provider agreements
- **Encryption and Security** for all data in transit

9.2 Transfer Safeguards

- End-to-end encryption for all international transfers
- Contractual data protection commitments from all processors
- Regular security assessments and compliance monitoring
- Ongoing adequacy evaluations and risk assessments

10. SECURITY MEASURES

10.1 Technical Safeguards

Data Protection:

- **Encryption in Transit:** TLS 1.3+ for all communications
- **Encryption at Rest:** AES-256 for all stored data
- **Database Security:** Encrypted databases with access controls
- **API Security:** OAuth 2.0 and secure authentication mechanisms

Infrastructure Security:

- **Network Protection:** Firewalls and intrusion detection systems
- **Access Controls:** Multi-factor authentication and role-based permissions
- **Monitoring:** 24/7 security monitoring and threat detection
- **Backup Security:** Encrypted backups with geographic distribution

10.2 Organizational Measures

Personnel Security:

- **Training:** Regular security and privacy training programs
- **Access Management:** Least privilege principles and regular reviews
- **Background Checks:** For employees with access to personal data
- **Confidentiality:** Binding agreements and data protection commitments

Vendor Management:

- **Security Assessments:** Comprehensive evaluations of all sub-processors
- **Contractual Requirements:** Data protection obligations in all agreements
- **Ongoing Monitoring:** Regular security reviews and compliance audits
- **Incident Coordination:** Coordinated response procedures

10.3 Customer Security Features

Account Protection:

- **Secure Authentication:** Multi-factor authentication options
- **Session Management:** Secure sessions with configurable timeouts
- **Access Monitoring:** Alerts for unusual access patterns
- **Data Controls:** Granular privacy settings and data sharing controls

Data Protection:

- **Secure Processing:** End-to-end encryption for all data processing
- **Export Security:** Secure data export with encryption and access controls
- **Deletion Verification:** Secure deletion with audit trails
- **Privacy Controls:** User-controlled privacy settings and preferences

11. CHILDREN'S PRIVACY

11.1 Age Restrictions

- AI Agents not intended for children under 13 (US) or 16 (EEA/UK)
- Business customers responsible for age verification where appropriate
- Enhanced safeguards for educational institution use
- Immediate deletion procedures for inadvertently collected children's data

11.2 Educational Use Considerations

Institutional Safeguards:

- Educational institutions responsible for student privacy compliance
- Enhanced privacy protections for student interactions
- Minimal data collection and processing for educational use
- Parental notification and consent procedures where required

11.3 Accidental Collection Response

- Immediate deletion upon discovery of children's data
- Parent/guardian notification where contact information available
- Process review and improvement procedures
- Documentation of incident response and corrective actions

12. DATA BREACH NOTIFICATION

12.1 Incident Response

Detection and Assessment:

- 24/7 monitoring and automated threat detection
- Rapid incident assessment and classification
- Immediate containment and mitigation measures
- Comprehensive investigation and impact analysis

12.2 Notification Procedures

Client Notification:

- Notification without undue delay upon incident confirmation
- Detailed incident information and potential impact assessment
- Assistance with Client notification obligations
- Regular updates throughout investigation and remediation

Regulatory and Individual Notification:

- Compliance with all applicable notification requirements
- Coordination with regulatory authorities
- Direct notification to affected individuals for high-risk incidents
- Ongoing cooperation with investigations and compliance efforts

13. POLICY UPDATES

13.1 Update Process

Regular Reviews:

- Periodic review and update of privacy practices
- Compliance monitoring for evolving legal requirements
- User feedback incorporation and best practice adoption
- Technology and service feature adaptations

13.2 Notification Methods

Advance Notice:

- Client dashboard notifications and alerts
- Email notifications to Client contacts
- Prominent notices on AI Agent interfaces
- Direct communication for significant changes

Material Changes:

- Extended notice periods for substantial changes
- Consent renewal requirements where legally required
- Opt-out options for new processing activities
- Clear documentation of changes and implications

14. CONTACT INFORMATION

14.1 General Inquiries

Widgera Inc. Privacy Team 1111B S Governors Ave #23248 Dover, Delaware 19904 United States **Email:** support@widgera.com

14.2 Privacy Rights Requests

Email: support@widgera.com **Subject Line:** "Privacy Rights Request - [Request Type]"

In-Chat Requests: Available for unregistered users directly through chat interface

14.3 Emergency Contact

Email: support@widgera.com **Subject Line:** "URGENT - Security Incident"

Response Timeframes:

- **Standard Requests:** 30 days for most jurisdictions
- **Urgent Deletions:** 24-48 hours for unregistered users
- **Security Incidents:** Immediate response and investigation

© 2025 Widgera Inc. All rights reserved.

This Privacy Policy was last updated on November 26, 2025.