Privacy Policy

January 20, 2026

Table of Contents

Guardian-X Privacy Policy

Effective Date: January 20, 2026 **Last Updated:** January 20, 2026 **Version:** 2.0

---

1. Introduction

Guardian-X Inc. ("Guardian-X," "we," "us," or "our") is committed to protecting your privacy and ensuring the security of your personal information. This Privacy Policy explains how we collect, use, disclose, retain, and safeguard your information when you use our emergency management platform and related services (collectively, the "Services").

This Privacy Policy applies to: - The Guardian-X Platform (iOS, Android, macOS, Windows, Apple Watch applications) - Administrative dashboards and web interfaces - Intelligence products (Guardian Recon, Guardian Sentinel, Guardian Horizon) - Our websites at guardianxi.com and related domains - All related services and communications

By using the Services, you acknowledge that you have read, understood, and agree to the practices described in this Privacy Policy. If you do not agree with this Policy, please do not use our Services.

---

2. Information We Collect

2.1 Information You Provide

Account and Profile Information - Name, email address, and phone number - Organization name and business information - Job title and role within your organization - Account credentials (passwords are securely hashed) - Profile preferences and settings

Emergency Alert Information - Alert type, content, and timestamps - Alert messages and descriptions - Response actions and acknowledgments - Incident notes and resolution information - Audio recordings (if voice recording features are enabled)

Payment Information - Billing address - Payment method details (processed by third-party payment processors) - Transaction history

Communications - Support requests and correspondence - Feedback and survey responses - Feature suggestions and enhancement requests

2.2 Information Collected Automatically

Device Information - Device type, model, and manufacturer - Operating system type and version - Unique device identifiers (device ID, advertising ID) - App version and configuration - Hardware settings and features

Location Information - Precise GPS location (during emergency alerts or as configured) - Approximate location based on IP address - Location history during active incidents - Geofencing zone entries and exits

Usage Information - Feature usage and interaction patterns - Session duration and frequency - Navigation paths and click patterns - Error logs and crash reports - Performance metrics and diagnostics

Network Information - IP address - Connection type (WiFi, cellular, ethernet) - Network carrier information - Browser type and version (for web interfaces)

2.3 Health and Biometric Information (Executive Protection Features)

If you use wearable device features, we may collect: - Heart rate measurements and patterns - Heart rate variability data - Fall detection events - Activity and movement data - Other vitals available through wearable APIs

Important: Health data is collected only with explicit consent and is used solely for executive protection and emergency alerting purposes. This data is encrypted in transit and at rest and is never sold or used for marketing.

2.4 Information from Third Parties

- Identity verification information from authentication providers
- Integration data from connected third-party services
- Publicly available information for intelligence products (OSINT)
- Threat intelligence from security data providers

---

3. Legal Basis for Processing (GDPR)

For individuals in the European Economic Area (EEA), United Kingdom, or Switzerland, we process personal data based on the following legal bases under Article 6 of the GDPR:

Purpose	Legal Basis
Provide and operate Services	Performance of contract
Emergency alerting and response	Legitimate interests; vital interests of data subjects
Account administration	Performance of contract
Customer support	Performance of contract; legitimate interests
Security and fraud prevention	Legitimate interests
Analytics and service improvement	Legitimate interests
Legal compliance	Legal obligation
Marketing communications	Consent (where required)
Health/biometric data processing	Explicit consent

Where we rely on legitimate interests, we have conducted a balancing test to ensure our interests do not override your fundamental rights and freedoms.

---

4. How We Use Your Information

4.1 Core Service Delivery

- Process and route emergency alerts to designated responders
- Enable real-time location tracking during emergencies
- Coordinate emergency response communications
- Authenticate users and manage account access
- Provide administrative dashboards and reporting

4.2 Service Improvement

- Analyze usage patterns to improve platform features
- Diagnose and fix technical issues
- Develop new features and capabilities
- Conduct research and analysis (using aggregated, anonymized data)

4.3 Safety and Security

- Detect and prevent fraud, abuse, and security threats
- Monitor for unauthorized access or suspicious activity
- Enforce our Terms of Service
- Protect the safety of our users and the public

4.4 Communications

- Send service updates and important notifications
- Respond to support requests and inquiries
- Deliver security alerts and account notifications
- Send marketing communications (with consent where required)

4.5 Legal and Compliance

- Comply with applicable laws and regulations
- Respond to legal requests and court orders
- Protect our legal rights and interests
- Support law enforcement investigations (as legally required)

---

5. How We Share Your Information

5.1 We Do Not Sell Your Personal Information

Guardian-X does not sell, rent, or trade your personal information to third parties for their marketing purposes.

5.2 Sharing Within Your Organization

Emergency alerts and related information are shared with designated administrators, responders, and contacts within your organization as configured by your organization's administrators. Your organization is the data controller for this sharing.

5.3 Service Providers (Subprocessors)

We share information with trusted third-party service providers who assist in operating our Services. These providers are contractually bound to: - Process data only as instructed - Implement appropriate security measures - Delete or return data upon termination - Not use data for their own purposes

Categories of Subprocessors:

Category	Purpose	Location
Cloud Infrastructure	Hosting and data storage	United States
Communication Services	SMS, voice, email, push notifications	United States

Category	Purpose	Location
Analytics	Usage analytics and performance monitoring	United States
Payment Processing	Subscription billing	United States
Customer Support	Ticketing and support tools	United States
Security	Threat detection and monitoring	United States

A complete list of subprocessors is available upon request at privacy@guardianxi.com.

5.4 Emergency Services

In life-threatening emergencies, we may share location and alert information with: - Police departments - Fire departments - Emergency medical services - Search and rescue organizations - Other first responders

This sharing is to facilitate rapid emergency response and protect the vital interests of individuals.

5.5 Legal Requirements

We may disclose information when required to: - Comply with applicable laws, regulations, or legal processes - Respond to valid legal requests (subpoenas, court orders, government requests) - Protect the rights, property, or safety of Guardian-X, our users, or the public - Enforce our Terms of Service - Investigate potential violations of our policies

We will provide notice of legal requests unless prohibited by law or court order.

5.6 Business Transfers

In connection with a merger, acquisition, bankruptcy, or sale of assets, your information may be transferred to the successor entity. We will provide notice before your information is transferred and becomes subject to a different privacy policy.

5.7 Aggregated and Anonymized Data

We may share aggregated, anonymized data that cannot reasonably be used to identify you for research, analytics, and benchmarking purposes.

---

6. Data Security

6.1 Security Measures

We implement industry-leading security measures to protect your information:

Technical Controls - Encryption in transit using TLS 1.3 - Encryption at rest using AES-256 - Regular vulnerability assessments and penetration testing - Web application firewall (WAF) protection - Intrusion detection and prevention systems

Access Controls - Role-based access control (RBAC) - Multi-factor authentication (MFA) for administrative access - Principle of least privilege - Regular access reviews and audits

Organizational Controls - SOC 2 Type II certified - ISO 27001 aligned security program - Employee background checks - Regular security awareness training - Incident response procedures

6.2 Data Breach Notification

In the event of a data breach affecting your personal information, we will: - Notify affected individuals without undue delay (within 72 hours for GDPR) - Notify relevant supervisory authorities as required - Provide information about the breach and remediation steps - Take immediate action to mitigate harm

---

7. Data Retention

7.1 Retention Periods

Data Type	Retention Period	Basis
Account information	Duration of account + 90 days	Service provision
Emergency alert records	7 years (configurable)	Legal compliance; audit requirements
Location data	Duration of incident + per retention policy	Emergency response
Usage logs	12 months	Security; analytics
Support communications	3 years	Customer service
Payment records	7 years	Financial compliance
Health/biometric data	90 days or as configured	Executive protection

7.2 Deletion

Upon account termination or valid deletion request: - Personal data is deleted or anonymized within 90 days - Backups are deleted according to backup rotation schedules - Some data may be retained as required by law or for legitimate business purposes

---

8. Your Privacy Rights

8.1 Rights for All Users

Regardless of your location, you may: - Access your personal information - Request correction of inaccurate information - Request deletion of your information (subject to legal requirements) -

Withdraw consent for optional processing - Contact us with privacy questions or complaints

8.2 Additional Rights for California Residents (CCPA/CPRA)

If you are a California resident, you have additional rights under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA):

Right to Know You may request information about: - Categories of personal information collected - Specific pieces of personal information collected - Sources of personal information - Purposes for collecting personal information - Categories of third parties with whom we share information

Right to Delete You may request deletion of your personal information, subject to certain exceptions (legal obligations, ongoing transactions, security, etc.).

Right to Correct You may request correction of inaccurate personal information.

Right to Opt-Out of Sale/Sharing Guardian-X does not sell personal information. We do not share personal information for cross-context behavioral advertising.

Right to Limit Use of Sensitive Personal Information You may limit the use of sensitive personal information to purposes necessary for providing the Services.

Right to Non-Discrimination We will not discriminate against you for exercising your privacy rights.

Financial Incentives We do not offer financial incentives for the collection of personal information.

CCPA Metrics: Information about consumer requests received and processed in the previous calendar year is available upon request.

8.3 Additional Rights for Virginia Residents (VCDPA)

Virginia residents have rights to: - Confirm whether we process your personal data - Access your personal data - Correct inaccuracies - Delete your personal data - Obtain a portable copy of your data - Opt out of targeted advertising, sale, or profiling

8.4 Additional Rights for Colorado Residents (CPA)

Colorado residents have similar rights to Virginia residents, plus the right to opt out of profiling in furtherance of decisions that produce legal or similarly significant effects.

8.5 Additional Rights for Connecticut Residents (CTDPA)

Connecticut residents have rights similar to Virginia residents under the Connecticut Data Privacy Act.

8.6 Rights for EEA, UK, and Swiss Residents (GDPR/UK GDPR)

You have the right to: - **Access:** Request a copy of your personal data - **Rectification:** Request correction of inaccurate data - **Erasure:** Request deletion (“right to be forgotten”) - **Restriction:** Request restriction of processing - **Portability:** Receive your data in a portable format - **Object:** Object to processing based on legitimate interests - **Withdraw Consent:** Withdraw consent at any

time for consent-based processing - **Lodge a Complaint:** File a complaint with your supervisory authority

8.7 Exercising Your Rights

To exercise your rights, contact us at: - **Email:** privacy@guardianxi.com

We will respond to verified requests within: - 30 days for GDPR requests - 45 days for CCPA/CPRA requests (extendable by 45 days with notice) - 45 days for state privacy law requests

We may need to verify your identity before processing requests. For requests submitted by authorized agents, we require proof of authorization.

---

9. Children's Privacy

Guardian-X is designed for enterprise use and is not intended for children under 16 years of age. We do not knowingly collect personal information from children under 16.

If you believe we have inadvertently collected information from a child, please contact us immediately at privacy@guardianxi.com. We will take steps to delete such information promptly.

---

10. International Data Transfers

10.1 Transfer Mechanisms

Guardian-X is based in the United States. If you access our Services from outside the United States, your information will be transferred to and processed in the United States.

For transfers from the EEA, UK, or Switzerland, we rely on: - **Standard Contractual Clauses (SCCs):** EU-approved contractual protections - **UK International Data Transfer Agreement (IDTA):** For UK transfers - **Swiss-U.S. Data Privacy Framework:** Where applicable

10.2 Data Processing Agreement

For customers subject to GDPR, CCPA, or other data protection laws, we offer a Data Processing Addendum (DPA) that governs our processing of personal data on your behalf. The DPA is available at guardianxi.com/legal/dpa or upon request.

---

11. Cookies and Tracking Technologies

11.1 Types of Cookies

We use the following types of cookies on our websites:

Type	Purpose	Duration
Essential	Authentication, security, session management	Session
Functional	Preferences, settings, language	1 year
Analytics	Usage statistics, performance monitoring	2 years
Marketing	Advertising effectiveness (with consent)	1 year

11.2 Managing Cookies

You can control cookies through: - Browser settings (block or delete cookies) - Our cookie preference center (where available) - Opt-out links for specific analytics providers

Note: Disabling essential cookies may affect the functionality of our Services.

11.3 Do Not Track Signals

Our websites do not currently respond to "Do Not Track" browser signals. However, you can control tracking through the methods described above.

11.4 Analytics

We use analytics services to understand how our Services are used. These services may collect information about your use of our Services and report trends without identifying individual users.

---

12. Automated Decision-Making

12.1 AI-Powered Features

Guardian-X uses artificial intelligence and machine learning in certain features, including: - Threat intelligence analysis and prioritization - Anomaly detection for executive protection - Report generation and summarization - Risk scoring for travel intelligence

12.2 Human Oversight

Automated systems are used to assist, not replace, human decision-making. For high-stakes decisions (such as threat assessments), human review is available upon request.

12.3 Right to Object

You have the right to object to solely automated decision-making that produces legal effects or significantly affects you. Contact privacy@guardianxi.com to request human review.

---

13. Third-Party Links and Services

Our Services may contain links to third-party websites or integrate with third-party services. This Privacy Policy does not apply to those third parties. We encourage you to review the privacy policies of any third-party services you access.

---

14. Changes to This Policy

We may update this Privacy Policy from time to time. When we make changes: - We will update the “Last Updated” date - For material changes, we will provide notice via email or through the Services - We will obtain consent where required by law

We encourage you to review this Privacy Policy periodically. Continued use of the Services after changes constitutes acceptance of the updated Policy.

---

15. Contact Us

If you have questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact us:

Privacy Inquiries Email: privacy@guardianxi.com

Data Protection Officer Email: dpo@guardianxi.com

General Contact Guardian-X Inc. A Virginia Corporation Email: support@guardianxi.com Website: https://guardianxi.com

EU Representative For GDPR inquiries from EU residents, contact: eu-representative@guardianxi.com

UK Representative For UK GDPR inquiries, contact: uk-representative@guardianxi.com

---

16. Additional Disclosures

16.1 Categories of Personal Information (CCPA)

In the preceding 12 months, we have collected the following categories of personal information:

Category	Examples	Collected	Disclosed
Identifiers	Name, email, phone, IP address	Yes	Yes
Customer Records	Account information, billing	Yes	Yes
Commercial Information	Transaction history, products purchased	Yes	Yes
Internet/Network Activity	Usage data, browsing history	Yes	Yes

Category	Examples	Collected	Disclosed
Geolocation Data	Precise location during alerts	Yes	Yes
Professional Information	Job title, employer	Yes	Yes
Biometric Information	Heart rate, vitals (if enabled)	Yes (consent)	No
Sensitive Personal Information	Account login, precise geolocation	Yes	Limited
Inferences	Preferences, behavior patterns	Yes	No

Sources: Directly from you, automatically through devices, from your organization, from third-party integrations.

Business Purposes: Service delivery, security, analytics, support, compliance.

Selling/Sharing: We do not sell or share personal information for cross-context behavioral advertising.

16.2 Your Organization's Role

When you use Guardian-X through your employer or organization: - Your organization is the data controller for Employee Data - Guardian-X acts as a data processor on behalf of your organization - Your organization's privacy policies also apply - Contact your organization's administrator for access, correction, or deletion requests

---

BY USING THE GUARDIAN-X SERVICES, YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTOOD THIS PRIVACY POLICY.

Version 2.0 - January 20, 2026