GermainUX Approach to Security and Compliance

Last Updated: 05/08/2025

Executive Summary

GermainUX is committed to delivering a secure, privacy-conscious, and compliant digital experience monitoring platform. Whether deployed on-premise or in the cloud, GermainUX incorporates strong security measures, data protection protocols, and internationally recognized compliance frameworks to safeguard customer data.

Data Security and Encryption

- **TLS Encryption** secures all data in transit over HTTPS (port 443).
- **Data at Rest** is encrypted across all GermainUX components.
- **Data Partitioning** ensures tenant isolation through logical separation.
- **Role-Based Access Control** ensures only authorized users can access data.
- **Support Access** is granted on a strict need-to-know basis and is fully auditable.

Data Privacy and Compliance

GermainUX aligns with global data privacy laws such as:

- **GDPR** (EU)
- **CCPA** (California)
- **LGPD** (Brazil)

We also implement:

- **Anonymization**: Strips identifiers while retaining analytical value.
- **Exclusion**: Omits sensitive fields via configurable rules.
- **Masking**: Obfuscates sensitive fields in real time.
- **PII Detection**: Uses AI to flag personally identifiable data.

Data Retention: Clients can configure retention up to 365 days and delete data on demand.

Monitoring, Auditing & Vulnerability Management

- **System Monitoring** and log analysis across all components.
- **Audit Logging** records all customer support access.
- **Vulnerability Scanning** runs weekly in CI/CD using OWASP Dependency-Check.

Deployment Options and Flexibility

GermainUX offers flexible deployment models:

- **On-Premise**: Full control over data and infrastructure.
- **Cloud (Hosted)**: Dedicated instances and data stores per client.

Both adhere to the same stringent compliance and security standards.

Third-Party Data Sharing

We share data only with authorized third-party service providers such as:

- Alchemer
- Verity Ascent
- Verifitech Info Pvt Ltd

All third-party relationships are governed by strong data protection agreements.

Customer Empowerment and Control

- **SMTP Configuration**: Clients can use their own SMTP for reports and notifications.
- **Usage Analytics**: Powered by Woopra; clients can disable tracking.

Governance

GermainUX enforces strict governance through:

- A formal Information Security Management System (ISMS) that guides all security efforts
- Internal ownership for risk, compliance, and control enforcement
- Documented governance structure and leadership accountability
- Ongoing audits and policy reviews to support SOC 2 readiness

Policies and Procedures

We operate with a robust set of policies for:

- Data collection, retention, and storage
- Access provisioning and monitoring
- Encryption, masking, and data exclusion

All policies are reviewed annually and acknowledged by employees

Certifications and Regulatory Compliance

GermainUX aligns with industry-leading standards and privacy regulations:

- **SOC 2 Type II**: Controls are evaluated annually to meet the Trust Services Criteria.
- **GDPR, CCPA, and LGPD**: Clients have tools to honor data subject rights, manage consent, and ensure data handling transparency.

We continuously review our program through internal audits and third-party assessments.

Infrastructure and Software

GermainUX includes:

- JS Script, Chrome Extensions, Mobile App, Dashboard, Agent, Engine, Enterprise Server
- Cloud deployments with encrypted data and logical partitioning

Business Continuity, Disaster Recovery, Incident Management

Our approach ensures operational resilience and responsiveness to incidents:

- **Business Continuity Plan** outlines recovery priorities and communication channels.
- **Disaster Recovery Plan** details procedures for restoring services across hosted and on-prem environments.
- **Incident Response Plan** includes preparation, detection, response, and post-incident review.
- Recovery Point Objective (RPO) and Recovery Time Objective (RTO) targets are defined based on client tier.

All plans are tested and updated annually.

Access Control

- Role-based access control (RBAC)
- Support access limited, time-bound, and logged
- Least privilege enforced across roles

Personnel Security

- All GermainUX employees undergo background checks as part of the onboarding process.
- Confidentiality and acceptable use agreements are required upon hire.
- Access is granted strictly on a need-to-know basis.
- Security awareness training is conducted annually, and specialized training is provided for sensitive roles.
- Internal access is logged, reviewed, and revoked upon role changes or separation.

Physical and Environmental Security

- **Cloud**: AWS data centers with world-class physical security
- **On-Prem**: Clients maintain their own physical security protocols

Encryption

- **In Transit**: All data in motion is secured with TLS 1.2 or higher.
- **At Rest**: Stored data is protected using AES-256 encryption standards.
- **Field-Level Controls**: Masking and exclusion are applied to sensitive fields.
- **PII Detection**: Integrated tools automatically flag high-risk fields for masking or exclusion.

Backup Policy

- GermainUX performs automated daily backups for all critical systems and customer data.
- **Standard backup retention** is 30 days, while **long-term archive backups** are retained for up to 365 days.
- **Audit records and security documentation** are retained for a minimum of 7 years to support compliance, litigation, and audit requirements.

Service and Availability

- Real-time monitoring and alerting
- Performance dashboards
- Client-configurable SMTP integration

Linked Policies

Refer to these foundational policy documents:

- Backup Policy
- Business Continuity Plan
- Data Classification Policy
- Data Protection Policy
- Data Retention Policy
- Disaster Recovery Plan
- Encryption Policy
- Incident Response Plan

For more information, visit: https://germainux.com