ProcessMind Enhanced Security Measures Overview

Effective starting: June 23, 2024

Introduction

Welcome to the ProcessMind Security Measures Overview. Committed to the highest standards of data protection, we ensure transparency and diligence in safeguarding your information. This document outlines our integrated security measures, designed to prevent unauthorized access, data breaches, and other threats. Our security framework combines sophisticated technical strategies with comprehensive organizational practices to ensure the utmost security of your data. For more details on our data protection efforts, please consult our Data Processing Addendum and Privacy Policy.

At ProcessMind, the security of your data is our top priority. We understand its value and guarantee that your data will never be sold to third parties. Our security infrastructure is reinforced with advanced technical and organizational measures, carefully crafted to protect your data at all times.

Technical Measures

Authentication: We employ industry-standard practices for secure access, including two-factor authentication (2FA) and the principle of least privilege. Single Sign-On (SSO) is facilitated through Microsoft Entra ID and Google OAuth/OICD, streamlining user authentication without the need for password storage.

Audit Trails: A centralized logging system records all system activities, enabling real-time monitoring and swift response to any irregularities. This practice is essential for maintaining security and compliance with regulatory standards.

Disaster Recovery Planning: Our disaster recovery strategy encompasses continuous data backups, multi-region database replication, and regular disaster recovery drills to ensure business continuity under any circumstances.

Continuous Security Monitoring: Through automated tools, we conduct comprehensive security scans of our infrastructure, adhering to best practices and compliance standards such as AWS security recommendations, HIPAA, NIST 800-53 rev 5, PCI DSS 3.2.1, and the OWASP top 10.

Regular Software Updates: We actively update our software packages to mitigate vulnerabilities, ensuring our systems are protected against known security threats.

Data Encryption: Our security strategy includes robust encryption for data in transit and at rest, preventing unauthorized access and ensuring the confidentiality of your information.

Secure Data Handling: Secure data upload mechanisms and the use of HTTPS across all services ensure the integrity and confidentiality of your data during transmission.

Data Isolation: Customer data is stored in dedicated databases to ensure security and privacy, minimizing risks associated with multi-tenant

environments. Shared resources are securely managed on a protected multi-tenant server.

Serverless Architecture: By adopting a serverless architecture, we significantly reduce the risk of server misconfiguration, enhancing our system's security against common vulnerabilities.

EU Data Storage Compliance: Customer data is securely stored in the EU (Frankfurt, Germany), complying with stringent EU data protection laws. Data is automatically deleted 30 days after contract termination to ensure privacy.

Segregated Accounts: We implement distinct accounts for routine operations and for accessing production environments. This approach minimizes the risk of inadvertently accessing or compromising Customer Data, in line with best practices for secure data management and access control.

Continuous Feature Verification: Our protocol requires ongoing verification of all features to ensure that updates do not compromise the integrity of our trust model. This rigorous testing process is crucial for maintaining the highest standards of reliability and security.

Organizational Measures

ISO27001 Certification: Our pursuit of ISO27001 certification demonstrates our commitment to international security standards, with a continuous commitment to achieve further certifications as dictated by our customers' needs.

Access Management: Through Active Directory, we ensure secure application access for employees via SSO, with MFA enforced to enhance security.

Role-based Access Control: We implement stringent role-based access control (RBAC) protocols for our employees, ensuring access to Customer Data is strictly limited to those with a need-to-know basis, in accordance with industry best practices for data security and privacy.

Security Consciousness: Our team is dedicated to security across all development processes. We regularly engage in discussions to enhance our security measures, creating an environment where security improvements are continuously identified and implemented.

Change Management Protocol: Our comprehensive change management protocol includes security considerations, ensuring that each modification undergoes a thorough security impact assessment. This process is aimed at maintaining the integrity and security of our systems, preventing any negative security implications with each change.

Feedback and Engagement: Customer feedback on our security practices is highly valued, playing a crucial role in our continuous improvement efforts to strengthen data protection.

At ProcessMind, our commitment to safeguarding your data is unwavering. We combine advanced technical safeguards with stringent organizational protocols to provide a secure, reliable service. Upholding data protection and privacy to the highest standards is our pledge to earn and maintain your trust.