ProcessMind SaaS Hosting

Effective starting: June 23, 2024

Introduction

ProcessMind B.V. (“we,” “us,” “our”) provides Software as a Service (SaaS) solutions hosted on Amazon Web Services (AWS) infrastructure located in *Frankfurt, Germany*.

This Hosting Policy outlines our commitments to our customers and the standards by which we operate to ensure the reliability, security, and compliance of our hosting environment.

Hosting Infrastructure

Our SaaS solutions are hosted on AWS, leveraging the robust, scalable, and secure infrastructure provided by Amazon Web Services. The primary data center location for our services is in Frankfurt, Germany, ensuring that your data is stored within the European Union (EU).

Data Security

We are committed to maintaining the security and integrity of our customers’ data. AWS provides a highly secure environment with a comprehensive suite of security services, including but not limited to:

- **Physical Security**: AWS data centers are protected by extensive physical security measures to prevent unauthorized access.
- **Network Security**: Advanced firewalls, intrusion detection systems, and encrypted communications ensure the security of data in transit and at rest.
- **Access Controls**: Strict access controls and authentication mechanisms are in place to ensure that only authorized personnel have access to customer data.

Data Privacy

Your privacy is important to us. We comply with all relevant data protection laws, including the General Data Protection Regulation (GDPR). For more details on how we handle your personal data, please refer to our Privacy Policy.

Service Availability

We strive to provide a highly available service. Our infrastructure is designed for redundancy and failover, ensuring minimal downtime. Our target uptime is 99.9% per month, excluding scheduled maintenance and force majeure events. See our Service Level Agrement for more information.

Backup and Disaster Recovery

- **Backups**: Regular backups of all critical data are performed to ensure data integrity and availability. Backup copies are stored in multiple locations to prevent data loss.
- **Disaster Recovery**: Our disaster recovery plan includes measures to restore services as quickly as possible in the event of a major incident. This includes regular testing of our recovery procedures to ensure effectiveness.

Compliance

Our hosting environment complies with the following standards and certifications, ensuring that our infrastructure meets stringent security and operational requirements:

- **ISO 27001**: Information Security Management
- **ISO 27017**: Cloud-Specific Controls
- **ISO 27018**: Protection of Personal Data in the Cloud
- **SOC 1, SOC 2, SOC 3**: Service Organization Controls
- **GDPR**: General Data Protection Regulation compliance for data protection and privacy

Customer Responsibilities

Customers are responsible for maintaining the security of their account credentials and for any actions taken using their accounts. Customers should:

- Use strong, unique passwords for their accounts.
- Regularly update and review access permissions.
- Immediately report any suspicious activity or security breaches to our support team.

Changes to Hosting Policy

We may update this Hosting Policy from time to time to reflect changes in our practices or legal requirements. We will notify customers of any significant changes through our website or direct communication.

Contact Information

For any questions or concerns regarding this Hosting Policy, please contact us at:

ProcessMind B.V.
Willem Sandbergstraat 33,
7425RC, Deventer,
The Netherlands
Phone: +31 85 060 68 09
Email: info@processmind.com

By using our services, you acknowledge that you have read, understood, and agree to be bound by this Hosting Policy.