Pre-Sales GA technical information

Security, Backup Data, SLA and Architecture

Contents

1. Security Policies

PortPal Solutions S.L. adheres to best practices in data security and privacy in compliance with the General Data Protection Regulation (GDPR) and other relevant European Union laws. The following security policies apply differently depending on the deployment model:

1.1 Data Encryption

For SaaS Customers:

All data is encrypted both at rest and in transit using industry-standard AES-256 encryption, leveraging cloud-based encryption services provided by our infrastructure providers. Data is stored in encrypted cloud storage across multiple availability zones for maximum security.

For On-Premise Customers:

Encryption methods are implemented using the customer's infrastructure. PortPal provides guidance on how to implement AES-256 encryption for both at-rest and in-transit data within the customer's network.

1.2 Access Control

For SaaS Customers:

Access to data is restricted based on roles and responsibilities. PortPal implements multi-factor authentication (MFA) and strict access control measures to ensure only authorized personnel have access to sensitive data. All access to the system is logged and monitored to detect unauthorized access attempts.

For On-Premise Customers:

Access control must be configured by the customer's IT team, with PortPal offering advisory services. MFA and strict role-based access should be implemented as per PortPal's recommended guidelines.

1.3 Security Monitoring and Incident Response

PortPal monitors all systems for suspicious activities using automated security tools. We employ

continuous monitoring and real-time alerts to detect and prevent potential breaches. In case of any security incident, PortPal has a robust incident response plan in place, including notification to relevant authorities and affected individuals in accordance with GDPR requirements.

1.4 Data Minimization and Retention

PortPal is committed to the principle of data minimization, ensuring that only the necessary personal data is collected and processed to deliver our services effectively. We retain personal data only for the duration required to fulfill the purposes for which it was collected, after which it is securely deleted.

This principle specifically applies to **transactional data** used for one-time processes such as document template generation, AI processing, and email generation. Such transactional data is utilized solely for the immediate purpose and is not stored beyond the completion of the transaction.

All other information accessible via PortPal is considered **non-transactional** and is retained in accordance with our data retention policies to facilitate ongoing services. This non-transactional data is handled with the utmost care to ensure privacy and security, adhering to all applicable laws and regulations and is treated in the next clause (2. Backup Data Policies) in this document.

2. Backup Data Policies

PortPal Solutions S.L. ensures the safety and integrity of data through regular backups. Our backup policies are designed to minimize data loss in the event of a system failure, cyberattack, or other disasters. These policies are in full compliance with European Union and United States regulations. Backup strategies vary between SaaS and On-Premise models:

2.1 Backup Frequency

For SaaS Customers:

Backups are performed every 24 hours at 1:00 a.m. GMT (UTC +0) and include all critical business and customer data. Full system backups are maintained on a rolling basis, ensuring that at least the last 30 days of data is always retrievable.

For On-Premise Customers:

Backup schedules need to be implemented by the customer's IT team based on their internal disaster recovery policies. PortPal provides recommended backup frequency guidelines and tools to facilitate backup processes.

2.2 Backup Storage and Security

For SaaS Customers:

Backups are stored in highly secure, geographically diverse data centers within the EU. Other data center locations can be explored by customer request. All backups are encrypted to the same standard as live data, ensuring protection in case of unauthorized access.

For On-Premise Customers:

Backup storage is handled by the customer's infrastructure. It is recommended to use encrypted storage devices and replicate backups to an offsite location for disaster recovery.

2.3 Data Restoration

In the event of a data loss incident, PortPal ensures that data can be restored within a maximum of 8 hours. Restoration processes are regularly tested to verify the integrity and availability of backups.

3. Service Level Agreement (SLA) and Technical Support

PortPal Solutions S.L. provides a comprehensive service level agreement for all its customers. This agreement outlines the availability of technical support and system uptime guarantees.

3.1 Uptime Guarantee

For SaaS Customers:

Our app ensures consistent performance with industry-leading uptime, providing a 99.9% uptime rate to minimize disruption to business operations. Scheduled maintenance is performed during off-peak hours with prior notification to clients.

For On-Premise Customers:

Uptime guarantees depend on the customer's hardware and network setup. PortPal provides support to ensure optimal configuration but cannot guarantee the same uptime as with the SaaS model.

3.2 Technical Support

PortPal provides a structured support framework to ensure that issues are addressed promptly based on their severity. Customers can reach out via email to support@portpal.me, except for Critical issues (P1), which can also be reported via phone directly with the Account Executive of assigned to the customer. The types of support levels and corresponding response times are defined as follows:

Critical (P1):

- Definition: Issues that cause a complete system outage or severe disruption of essential business operations (e.g., system crash, data corruption).
- Response Time: Within 1 hour, 24/7 (including weekends and holidays).

High (P2):

- Definition: Issues that impair system functionality but allow for partial operations (e.g., degradation of performance, limited feature availability).
- Response Time:
    - During office hours: Response within 4 hours.
    - Out of office hours: Response within the day.

Medium (P3):

- Definition: Issues that cause minor disruptions or inconveniences but do not significantly impact business operations (e.g., a single feature not working as intended).
- Response Time:
    - During office hours: Response within 24 hours.

- Out of office hours: Response within the next business day.

Low (P4):

- Definition: Non-urgent issues such as general inquiries, feature requests, or cosmetic bugs that do not impact operations.
- Response Time:
  - During office hours: Response within 48 hours.
  - Out of office hours: Response within the next 3 business days.

Office Hours:

PortPal's standard office hours are from 9:00 am to 18:00 pm, GMT+1, Monday through Friday, excluding public holidays.

Out of Office Hours

Issues reported outside standard office hours will be handled based on the priority level as described above.

3.3 Root Cause Analysis (RCA)

For any critical incidents that impact service availability, PortPal provides a Root Cause Analysis (RCA) report within 5 business days of the incident resolution. This report details the cause of the issue, the actions taken to resolve it, and any preventive measures implemented.

4. SaaS Architecture

4.1 Overview

PortPal's SaaS solution is fully hosted on cloud platforms, leveraging distributed systems and cloud-native services to provide high availability, scalability, and security.

4.2 Components

- **Application Layer:** Hosted in a multi-tenant environment, with resource isolation for each

customer.

- **Data Storage:** Data is stored in cloud databases that are encrypted and automatically backed up across multiple data centers.
- **Security:** All traffic to and from the application is encrypted using TLS. Centralized access management and security monitoring ensure compliance with industry standards.

5. On-Premise Architecture

5.1 Overview

For customers requiring an On-Premise installation, PortPal's solution is deployed within the customer's local data center. The customer has full control over the hardware and software environment, ensuring compliance with internal policies.

5.2 Components

- **Application Layer:** Installed on customer-provided hardware. PortPal offers guidance on system requirements and best practices for configuration.
- **Data Storage:** Data is stored locally on customer-managed servers. Backup and recovery procedures are under the customer's control, with PortPal providing tools for local encryption and storage.
- **Security:** The customer is responsible for implementing network security, including firewall configurations and access control policies. PortPal offers support and recommendations to meet security standards.