Pace

The agentic process outsourcer for insurance

Data Security Overview

CONFIDENTIAL

Pace | Built for the world's largest insurers

At Pace, we take data security and privacy extremely seriously. We understand that our customers deal with sensitive customer data including Protected Health Information and are committed to providing robust security measures to protect their data.

See an overview of our security and privacy policy here: https://withpace.com/security. We are also SOC 2 Type II compliant - see the full security audit report here: https://trust.withpace.com/.

Contents	Page #
Overview	2
Data Storage and Handling	4
Controls	9

CONFIDENTIAL

Industry Leading Compliance



SOC II



CCPA



GDPR



Granular permissions

Secure authentication with SSO, role-based access controls, and audit logs



Compliant data residency

Industry standard HIPAA and GDPR policies and support for self-hosted deployments



Enterprise-grade privacy

Never train on your data



Dedicated security professionals

White glove support from our in-house security team

Access the Pace Trust Center

CONFIDENTIAL

Data Storage and Handling

CONFIDENTIAL

Handling and Storing Data

Storage Location		We utilize Amazon Web Services (AWS) for storing data. Data is encrypted at rest and in transit
Data Retention		We support Zero Data Retention for our LLMs via our OpenAI partnership or Azure OpenAI. Learn more about Zero Data Retention here
Data Usage		We never use any of customer data for training purposes unless it is with the customer's explicit permission for improving their own models
PII/ PHI Handling		While our existing data encryption policies are typically sufficient for meeting GDPR compliance, we also offer specific handling of PII data. There are two options: • **Redaction API**: Customer provides a redaction service which we will integrate with. This is the recommended approach. • **Custom**: We can build out redaction on your behalf, but this will impact the speed and accuracy of the system and increase time to go live and platform cost. We typically do not recommend relying on our system for redaction, so reach out if you're considering this option.

Encrypted at Rest and in Transit

Encryption at Rest

All data stored in AWS S3 is encrypted at rest using industry-standard encryption algorithms. This means that even if unauthorized individuals were to gain access to the stored data, they would not be able to decipher it without the proper encryption keys

Encryption in Transit

We employ encryption protocols to protect data in transit. All communication between our systems and the data storage is conducted over secure channels using encryption mechanisms such as SSL/TLS. This ensures that data remains confidential and tamper-proof during transmission

Certifications

Independently Verified



SOC II



CCPA



GDPR

SOC II: We have completed our SOC 2 Type II process. Please reach out to receive the report. This rigorous certification demonstrates our commitment to maintaining a secure and reliable system. It involves a comprehensive audit of our security controls, policies, and procedures by an independent third party. The American Institute of Certified Public Accountants (AICPA) developed SOC 2 around five Trust Services Criteria: security, availability, processing integrity, confidentiality, and privacy

GDPR: We are GDPR compliant and support the deletion of any data upon user request.

PIPEDA: Pace's controls and policies are in line with PIPEDA standards for our Canadian partners

CONFIDENTIAL

Choose your deployment options

Multi-Tenant

Our standard cloud deployment:

- Fully managed
- Scalable
- Cost-efficient

Hosted on AWS through Render, this option provides fast setup, automatic scaling, and ongoing maintenance with strong logical data isolation between customers

This is our recommended and most commonly adopted approach

Most Common

Single-Tenant

A dedicated environment for your organization, deployed in the region of your choice

Provides complete data isolation, customizable configurations, and stronger compliance controls.

Compared to our Multi-Tenant option, this approach increases time to go live and overall platform cost

Reach out if you're considering this option

On-Premise/BYOC

Deploy the platform directly within your cloud or on-premises infrastructure

You retain full control of your data, networking and security policies, while we handle deployment, monitoring, and updates

Compared to our Multi-Tenant option, this approach will greatly increase time to go live and overall platform cost

Reach out if you're considering this option

Controls

CONFIDENTIAL

Infrastructure (1 of 2)

Encryption key access restriction	The company restricts privileged access to encryption keys to authorized users with a business need
Unique account authentication enforced	The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys
Production application access restricted	System access restricted to authorized access only
Production database access restricted	The company restricts privileged access to databases to authorized users with a business need.
Firewall access restricted	The company restricts privileged access to the firewall to authorized users with a business need.
Production OS access restricted	The company restricts privileged access to the operating system to authorized users with a business need.
Production network access restricted	The company restricts privileged access to the production network to authorized users with a business need.
Unique network system authentication enforced	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.
Remote access encrypted enforced	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.

CONFIDENTIAL

Infrastructure (2 of 2)

Log management utilized	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives
Infrastructure performance monitored	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met
Network segmentation implemented	The company's network is segmented to prevent unauthorized access to customer data
Network firewalls reviewed	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion
Network firewalls utilized	The company uses firewalls and configures them to prevent unauthorized access
Network and system hardening standards maintained	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually

CONFIDENTIAL

Organizational Security

Employee background checks performed	The company performs background checks on new employees
Confidentiality Agreement acknowledged by contractors	The company requires contractors to sign a confidentiality agreement at the time of engagement
Confidentiality Agreement acknowledged by employees	The company requires employees to sign a confidentiality agreement during onboarding
Performance evaluations conducted	The company managers are required to complete performance evaluations for direct reports at least annually
Password policy enforced	The company requires passwords for in-scope system components to be configured according to the company's policy
MDM system utilized	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service

CONFIDENTIAL

Product Security

Data encryption utilized	The company's datastores housing sensitive customer data are encrypted at rest
Control self-assessments conducted	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA
Penetration testing performed	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs
Data transmission encrypted	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks
Password policy enforced	The company requires passwords for in-scope system components to be configured according to the company's policy
Vulnerability and system monitoring procedures established	The company's formal policies outline the requirements for the following functions related to IT / Engineering: • Vulnerability management • System monitoring

CONFIDENTIAL

Internal Security Procedures (1 of 3)

Cybersecurity insurance maintained	The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions
Configuration management system established	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment
Whistleblower policy established	The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns
Board oversight briefings conducted	The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed
Board charter documented	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control
Board expertise developed	The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed
Board meetings conducted	The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company

CONFIDENTIAL

Internal Security Procedures (2 of 3)

System changes externally communicated	The company notifies customers of critical system changes that may affect their processing
Organization structure documented	The company maintains an organizational chart that describes the organizational structure and reporting lines
Roles and responsibilities specified	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy
Support system available	The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel
System changes communicated	The company communicates system changes to authorized internal users
Access requests required	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned
Incident response plan tested	The company tests their incident response plan at least annually
Company commitments externally communicated	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS)

CONFIDENTIAL

Internal Security Procedures (3 of 3)

External support resources available	The company provides guidelines and technical support resources relating to system operations to customers
Service description communicated	The company provides a description of its products and services to internal and external users
Third-party agreements established	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity

CONFIDENTIAL

Data and privacy

Customer data deleted upon leaving	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.

CONFIDENTIAL