check-in pax

Security Whitepaper

v6.0

Explore the comprehensive data security framework of Check-in Pax, safeguarding the integrity of event planners' data and operations.

For more detailed information please refer to our information security policy.

> Our team has invested significant time and resources in developing Check-in Pax, which meets some of the highest compliance standards. By prioritizing strong data security throughout the event cycle, we are proud to provide a secure environment for event planners to create unforgettable event experiences
>
> **Oliver Davis**
> Head of Product

NOTE:

Check-in Pax also offers a lightweight version that can be used with limited to no personal identifiable data.

This allows for a faster compliance process.

GDPR-compliant

Learn more

Transparent DPA

Download DPA

Concise Terms of Service

Compliant Privacy Policy

Security & privacy by design

Certified and scalable infrastructure:

Check-in Pax utilizes Amazon Web Services (AWS) to provide you with robust security and flexibility when scaling up.

Data Encryption:

All data is stored in an encrypted database at rest (AES-256) and transmitted in transit via SSL/TLS.

Data Storage:

Data storage options in the US, EU, and Asia are available upon request. We recommend selecting the storage option that is geographically closest to your events for optimal performance.

Certified Security:

We conduct regular audits and penetration tests for our Apps and API to help identify and address vulnerabilities and safeguard our systems and data.

99.9%

UPTIME

With a 99.9% uptime, our focus is on maintaining continuous service without interruptions.

View status page

Data Deletion

To address the security risks associated with obsolete data in the system and In compliance with GDPR's right to be forgotten' principle, we offer the option to delete/purge all guest list data from our servers, ensuring the complete removal of personal identifiable information.

The following information from a deleted event will be permanently purged (irreversible deletion of data) from the database and server, making this data unrecoverable:

- All guest details including name, company, and other personal information
- All guest images
- All guest PDF badges
- Guest check-in logs
- Event's email templates
- Event's email logs
- Guest list Excel or CSV files through which the guest list was imported
- If team members were added previously, the event is also automatically unassigned from other team member's accounts and therefore made inaccessible.

You're always in control

Your Guests, Your Data

Your guests' data privacy is our utmost concern. We never use or share your guest data. It's important to note that our customer support team does not have access to your guest lists as access is technically restricted. Access is only possible with your explicit permission.

Guest Data Selection

Take ownership of your data by defining the guest fields you wish to utilize and display in the app. We process only the data you create, putting you in control of customizing and managing your event information.

Guest Communication Oversight

With features like invitation management and QR code confirmations, you are in charge of every guest communication. Nothing is sent to guests automatically by the system, ensuring that you oversee and control all interactions throughout the event.

Compliance Readiness Checklist

We understand that event planners operate under tight deadlines. To streamline compliance and on-boarding processes, we have curated this comprehensive checklist.

Infrastructure & Network Security

Amazon Web Services
Check-in Pax uses AWS for cloud infrastructure.

Anti-DDoS attacks
Protection against Distributed Denial of Service (DDoS) attacks is ensured through AWS Shield.

Infrastructure Security
Remote users are required to connect to the cloud infrastructure using a VPN with MFA enabled.

Separate UAE/Staging and Production Environment
Check-in Pax maintains separate/isolated environments for Development, Staging and Production/Live environment.

Web Application Firewalls (WAF), Fraud & Bot Control
We leverage AWS WAF for web application firewall protection, safeguarding our web applications from common exploits that could impact availability, compromise security, or consume excessive resources. Our Fraud Control features Managed Rules on AWS to protect login and sign-up pages from fraudulent activities, while Bot Control utilizes Managed Rules for visibility and control over prevalent bot traffic.

IDS/IPS and SIEM
Currently, we do not utilize any IDS or SIEM tools. We may consider implementing these tools in the future if recommended by our information security team.

Business Continuity and Disaster Recovery Plan for SaaS
We have a robust business continuity plan tailored to our Software as a Service (SaaS) business model, ensuring seamless operations and service availability in the event of disruptions.

Regular Penetration & Vulnerability Assessments
We conduct regular penetration testing and vulnerability assessments across our applications, systems, and infrastructure. The documented Disaster Recovery and Business Continuity Plan is reviewed annually. The infrastructure is designed with high availability and redundancy in mind.

Wireless Security
Our wireless networks are protected using WPA2 and strong password protection. Strong passwords typically consist of a combination of uppercase and lowercase letters, numbers, and special characters. Additionally, they should be at least 12 characters long and unique for each Wi-Fi device.

Data Security

Access Monitoring
Internal access logs and permissions are reviewed on a regular basis to identity unauthorized activity and unnecessary permissions.

Data Isolation
We implement data segregation in our multi-tenant SaaS system through separate data tables for user accounts and their associated events, along with role-based access control to ensure appropriate data access levels for each client.

Data Backups
For data security and backups, we implement regular regional backups to safeguard against potential data loss, utilizing AWS Backup for EC2 instances and automated RDS backups for our database.backups are created on a regular basis in the event of an incident that results in data loss.

Data Deletion
When a user initiates the deletion process through the functions such as delete guest, delete guest list, delete event, and delete account, we ensure the complete removal of personal identifiable information by purging all guest list data from the servers. This aligns with GDPR's 'right to be forgotten' principle.

Encryption in transit
"All Check-in Pax traffic for both the website and application is encrypted in transit using Transport Layer Security (TLS) 1.2 with an industry-standard AES-256 cipher for secure communication.

Encryption at Rest
All our databases are encrypted with the AWS
Database Encryption SDK that uses an algorithm suite with AES-GCM, an HMAC-based extract-and-expand key derivation function (HKDF), HMAC verification, ECDSA digital signatures, key commitment, and a 256-bit encryption key.

Event Logging and Review
We implement logging to capture internal events, which are periodically reviewed to ensure security and compliance with established protocols.

Password Security
Check-in Pax employees are required to create strong passwords for internal accounts. MFA and SSO are to be used where supported.

PCI DSS
Check-in Pax uses Stripe to charge credit cards and by doing so do not have access to the user's credit card details. We use best practice integrations by Stripe to collect payment information.
More information here: https://docs.stripe.com/security/guide

Product Security

Comprehensive security features to help event teams protect their guest data:

Audit Logging
The Check-in Pax platform includes audit logs so admins can gain visibility into user and team member activities including but not limited to last login, user access rights, guests created, guests modified, and guests checked-in.

Advanced Security Measures: reCAPTCHA v3 Implementation
We use reCAPTCHA v3 for all our application's login and sign-up pages as an additional layer to help protect us from spam and password decryption. This new version uses advanced behavioral analysis to distinguish between actual users and automated bots, hence preventing abusive traffic without requiring any user interaction.

Role-Based Access Control
At Check-in Pax, we prioritize the implementation of role-based access control (RBAC) as a fundamental principle across all aspects of our operations. RBAC ensures that access to systems, data, and resources is granted based on predefined roles and responsibilities, aligning with the principle of least privilege.

Session Time Out
Access to the Check-in Pax event management platform will automatically time out after 60 minutes of inactivity.

Strong Password Policies.
Our enterprise-ready and configurable password policy requires users to create passwords that are at least 8 characters long, include a mix of letters, numbers, and special characters with the option to enforce a password change at intervals of 90 days, 6 months, or as needed.

Multi-Factor Authentication (MFA) with One-Time Passwords (OTP)
Our system employs Multi-Factor Authentication (MFA) using One-Time Passwords (OTP) to enhance security during the login process, ensuring that user accounts are protected from unauthorized access.

SSO Support
Coming soon: Enterprise customers can authenticate to Check-in Pax using their existing SSO idP.

Data Logging and Sensitive Information Protection
Sensitive information is not printed or stored in logs to ensure confidentiality and security.

User Credential Security
User credentials are encrypted and hashed with random salt to ensure secure storage.

API Security
By default, the API access token has a lifetime of 30 days. After the token expires, users will be automatically logged out to maintain security.

Application Security

Credential Management
User passwords are salted and hashed before storage.

Key Management
All data at rest for both RDS and EC2 EBS volumes is encrypted using the AWS Key Management Service (KMS).

Restricted IP Address Policy
We restrict access to a very limited set of IP addresses for developers to access the system.

Software Development Lifecycle
Check-in Pax Secure Development Lifecycle Standard requires the following: Planning and documentation, Peer review, Testing in pre-production documents, User acceptance testing, Version control for all code changes

Vulnerability & Patch Management
Vulnerabilities are addressed within a predefined SLA that considers their severity.

Secure Software Development Practices
In our secure software development practices, we adhere to industry best practices by implementing secure coding standards, conducting regular security reviews, and performing thorough testing throughout the development lifecycle. Additionally, we enforce a strict separation of production systems and data from live systems, requiring approval before any changes are made.

Incident Reporting
In the event of a data breach, we will immediately initiate our incident response plan, notify all affected parties within 48 hours, and work swiftly to contain and resolve the breach to minimize impact.

UAT Testing
We conduct user acceptance testing (“UAT”), load testing, and stress testing at the final stage of the development lifecycle for new releases to ensure the robustness and security of the system.

Employee Security Training
We provide regular security training sessions for employees to ensure they are equipped with the knowledge and skills to maintain a secure work environment. These training sessions cover best practices in data protection, threat awareness, and incident response protocols, reinforcing our commitment to upholding the highest standards of security within our organization.

Policies

Request access

Check-in Pax uphold the following internal policies for security and compliance.

Information Security Policy

- **Password Policy**
- **Incident Response Policy**
- **Business Continuity/Disaster Recovery (BC/DR) Policy**
- **Software Development Lifecycle Policy**
- **Supplier Code of Conduct Policy**
- Acceptable Use Policy (AUP)
- Remote Work & BYOD (Bring Your Own Device) Policy
- Cloud Security Policy
- Encryption Policy
- Employee Training & Awareness Policy

Access Our Essential Legal Documents:

Privacy Policy, Terms of Service, and Data Processing Agreement

Privacy Policy

Data Processing Agreement (DPA)

Terms of Service

check-in pax

More questions about security & privacy?

Get in touch.

Our security team is on a standby to answer all your questions.

Contact us

checkinpax.com

privacy@checkinpax.com