Data Security Overview

Classification: Public

About this Document

This document contains an overview on information and data security practices for Groupize and the Groupize event management application. It is intended to provide the initial information most commonly requested by our customers when conducting a security and data privacy analysis of Groupize.

Compliance and Audit

Groupize is ISO 27001 and PCI DSS 3.2.1 certified.
The following areas were evaluated:

- Network and Systems Security
- Cardholder Data Protection (including PII)
- Vulnerability Management and Remediation
- Access Control Management
- Network and Security Monitoring
- Information Security Policy
- Organizational Processes and Controls

PCI Audit is completed annually by our partners at Security Metrics[1]. We are audited against the SAQ D - Service Providers standard. We are happy to provide our PCI Attestation of Compliance on request.

ISO 27001 certification was achieved in 2022 by Aprio[2]. This is the world's most prestigious international standard for information security management system ("ISMS") certification demonstrating the highest level of internal compliance and security.

Hosting and Physical Security

Groupize is primarily hosted by Heroku, a Platform as a Service provider that is owned and operated by Salesforce. Heroku, in turn, hosts their physical infrastructure with Amazon Web Services.

Heroku is also PCI, ISO and SOC 2 compliant in addition to a number of additional compliance standards. AWS maintains similar standards.

We utilize Heroku's Enterprise-level Shield[3] service to ensure that all Groupize-housed data is independent of other Heroku customers and run in an isolated environment. This is true of all of our environments (testing, staging and production). This configuration has been considered as part of our

[1] https://www.securitymetrics.com/
[2] https://www.aprio.com/
[3] https://www.heroku.com/shield

PCI DSS audit and our independent auditors have verified that it meets the standards necessary to provide a high standard of security.

On occasion, as part of a security screening, we are asked about topics like:

- Intrusion detection
- Operating System updates and patches
- Firewall configuration
- Application deployment and separation of responsibilities
- Technical access and audit logging

For each of these topics services are provided by Heroku to archive best practices. In some cases, such as operating system patching, Heroku provides a fully managed service and Groupize staff simply is not involved in that process. For others, like audit logging and deployment, heroku provides tooling to facilitate those efforts and Groupize staff uses the Heroku provided tooling.

The details of some of these services - such as security configurations, vendors, and firewall configurations - are confidential. As a matter of policy Heroku does not make that information available. Details on Heroku and AWS's independent audit certifications are available, however, and those certifications serve as assurance of compliance with these standards.

As Heroku is ultimately hosted by Amazon Web Services (with our current data center being, exclusively, Amazon's us-east-1 data center in Virginia, USA) all physical security is the responsibility of Amazon. Accordingly Amazon does not allow individuals to tour or inspect their data centers.

Additional Vendors and Services

In addition to Heroku, Groupize utilizes a number of additional services that may house, temporarily or permanently, customer data. For a full list please see our subprocessor documentation (available on request). The following are a few common services that our customers ask about:

- **Amazon Web Services (directly):** In addition to our use of AWS through Heroku we also directly use AWS S3 for file storage and AWS KMS for encryption key management and data encryption services. KMS usage for a Groupize customer is limited to those customers who choose to enable credit card collection on their accounts. S3 hosting is used for storing uploaded files such as data import spreadsheets, images, videos and any other content used to customize a customer's events.
- **Filepicker by Filestack:** Filepicker is a service provided by the company filestack that allows us to provide a rich and interactive user interface for customers who are uploading images, video, or other media content. Files of these types are first uploaded to filestack, who process the media (resizing, cropping or otherwise manipulating the media to fit the needs of the application) and then Filestack uploads the various versions of the media to Groupize's Amazon S3 bucket. This means that customer files can, for some short period of time, live on Filestack servers while they are being formatted.
- **Userpilot:** Groupize utilizes to provide support to our customers including tips, onboarding tutorials, and new feature notifications. Additionally this tool measures feature usage and value.

Data Security and Personally Identifiable Information

In order to successfully plan an event Groupize must collect some personally identifiable information from each attendee. Additionally we require a small amount of information from our users (planners and event professionals). At present our only required PII is

- First Name
- Last Name
- Email Address

We provide event planners the ability to request or require additional information as part of the event registration process and planners are allowed to specify their own, custom fields, for collection.

Planners are given the option to provide their own terms and conditions as well as a GDPR data collection and privacy statement to align with the data they choose to collect.

For the purposes of booking travel we may need to collect additional information.

If an attendee is booking a live hotel room we are required to collect the phone number of the primary occupant of the room as well as payment details for purposes of either charging, or placing a guarantee, against the room.

If an event is connected to SAP Concur we may collect the users SAP Concur login ID and aggregate additional travel information in order to generate a unified itinerary.

In the event that a payment is being processed Groupize supports three mechanisms of payment processing:

- For live hotel bookings all payments are processed by our partner Travelport who provides a connection to the various hoteliers reservation systems. Groupize transmits payment data, and required booking information, to Travelport and receives a confirmation number. For this workflow we never store payment details, with the exception of the last 4 digits of the card that is used, and the cardholder name.

- For purchases through our Ticketing feature we integrate with Stripe payment processing. The Groupize customer's Stripe account is used to enable this service - no payments are processed by Groupize directly. We do not store any payment information other than the stripe-returned confirmation code.

- For users of our verify card service we encrypt and temporarily store credit card information. A Groupize customer must opt-in to using this service and card data is purged as soon as it is no

longer relevant for an event. This service has been fully vetted by our PCI Auditors for security and compliance with PCI standards.

Data Encryption and Transport

All Groupize data is encrypted at rest as part of our Heroku Enterprise Postgres database service[4]. Data related to our verify card service is further encrypted via Amazon KMS using AES 256 level encryption. Groupize does not store or manage the encryption keys - those are managed by KMS. When in transit all data is secure via TLS 1.2 or higher encryption.

Access - Authentication and Authorization

Groupize users authenticate to the system in one of two ways.

The primary mechanism is via a username and password. Passwords are stored in the Groupize database, salted and hashed using the bcrypt utility. We adhere to PCI DSS requirements for password management including requiring strong passwords that expire every 90 days. User accounts are disabled after a number of invalid attempts to access the system and must be unlocked by a Groupize support administrator.

Optionally, customers can enable Single Sign On via the SAML 2 standard against their own identity management system. This feature is available on request to Groupize Customer Success and may require an additional support fee.

Role Based Security

Within the Groupize system access to events and data can be configured based on a number of predefined roles. Groupize customer accounts are divided into multiple organizations (generally representing different divisions of a company or other logical real-world structure).

A user can be designated as a member of an organization, member of an account, admin of an organization and/or account or the owner of an account. The permissions are as follows:

Member - members can create their own events in either the account or organization they belong to and fully manage those events. They cannot see any other events unless another planner adds them to the event as a “collaborator”.

Admin - Admins can fully see and manage any events in the organization and/or accounts they are an admin of. An admin can be an admin of one organization and not another - allowing them to see only

---

4 https://devcenter.heroku.com/articles/heroku-postgres-production-tier-technical-characterization#data-encryption

those events relevant to their position. Admins can also add / manage users of their organization and/or account.

Owner - An account owner has full control over the Groupize account and cannot be removed by another admin. To be removed this user must reassign ownership to another user or Groupize support can assist in the event that the original owner is no longer available.

Attendees - Finally an individual can be an attendee of an event. Attendees are not a conventional “user” in that they have no username or password and cannot log into Groupize. They have access to view or modify their specific registration of an event. An attendee of one event is not directly associated with any other event - even if it is the same person.

System and Support Access

Groupize customer success & support, and Groupize engineering have access to the application on a “as required” basis to support our customers and ensure ongoing operations. This means that some Groupize employees may be able to see user or attendee information in order to do their jobs or ensure that the system is running smoothly. All Groupize employees agree to an information security policy that requires that this access only be used in direct service of a customer or to support / resolve an operational problem. Employees who violate this policy face sanction up to and including termination. This policy also prohibits employees from downloading, transporting or otherwise disseminating any customer data outside of approved mechanisms and systems including downloading data to physical media or personal accounts.

Technical access to our servers (Heroku, AWS) is managed by those respective providers’ authentication and authorization systems and is audited quarterly or whenever there is a change in employment status for any privileged employee (whichever is more often).

In some cases system-to-system access is provided to support application operations. This includes the previously mentioned services like Filestack, which has access to Groupize’s AWS S3 file storage for the purpose of uploading processed files. No third party vendors directly access Groupize-hosted data in a non-electronic fashion unless directly requested to do so by a Groupize employee who is pursuing resolution of a system issue (for example, we may allow a Heroku support engineer to access our account if needed to resolve a hosting issue, but they are required to explicitly seek permission first).

Conclusion

At Groupize managing our customer data, safely and securely, is among our highest priorities. Hopefully the information in this guide provides the fundamental understanding of how we achieve that objective. Should you have any additional questions about Groupize security please contact your customer success or sales representative, or Groupize-partner travel management contact.