Groupize - GDPR Annex II Controls

Measures of pseudonymisation and encryption of personal data

- All data in the system is encrypted at rest utilizing AES-256 encryption block-level encryption[1]
- When attendee information is communicated to third party data processors, or used for reporting purposes, the attendee ID is utilized - unless the PII is necessary to perform a task in interest of facilitating a meeting or event.
- All transfers of data both internally and externally occur over TLS 1.2 or higher encrypted communications.
- Additional sensitive information is column-level encrypted via AWS KMS using AES-256 encryption.[2]

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- The Groupize application is hosted on Salesforce Heroku's Enterprise tier service which includes multiple availability zones to ensure availability as well as dedicated servers and isolated networks to ensure confidentiality.
- Regular monitoring is in place to alert engineering and support staff of any issues with system resilience, including built-in Heroku monitoring as well as error reporting through Rollbar.
- Integrity is controlled via restricted role access, authentication and authorization systems and limited direct access to back-end systems. This prevents modifications to data that are unintentional or undesired.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- All data is backed up on a continuous basis, with a week of archives available. This backup process is managed by Salesforce Heroku directly and Groupize staff do not have direct access to the backups, senior engineering staff can, however, trigger a recovery as needed.
- Backup restoration tests are conducted twice a year to verify this process.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

---

[1] https://devcenter.heroku.com/articles/heroku-postgres-production-tier-technical-characterization
[2] https://aws.amazon.com/kms/

- Groupize conducts a full annual evaluation of every Information Security Management System (ISMS) control, policy and procedure. This is independently audited by Aprio for ISO/IEC 27001 certification.
- Additionally application development includes multiple tests of controls including code review, automated test execution before deployment, automated security vulnerability and static code analysis before deployment
- Groupize conducts monthly automated external penetration tests on the system and hosting environment and an annual manual penetration test. This is conducted by Security Metrics.
- Annual disaster recovery and business continuity planning tests are conducted.

Measures for user identification and authorisation

- All users are authenticated in one of three ways:
    - Via Single Sign On over a SAML2 connection to the Groupize customer's Identity Provider. This is applicable to event planners.
    - Via Username and Password persisted to the Groupize application database. All passwords are bcrypt hashed and salted and all accounts must adhere to a password policy that includes strong password requirements and periodical password changes. This is applicable to event planners.
    - Via a dynamically generated access token appended to a link in a registration confirmation email. This only applies to event attendees and only provides them access to the specific event for which they have registered. Attendees cannot view other events or other attendee information using this link.

Measures for the protection of data during transmission

- All data transmission occurs over TLS/SSL utilizing TLS 1.2 or higher.

Measures for the protection of data during storage

- All data is encrypted at rest via AES-256 encryption. While data hosting is through Heroku Postgres they subcontract the physical hosting and storage to Amazon Web Services utilizing their RDS product.
- All data is backed up using Heroku's continuous protection service which provides a rolling 7 day window to back up data to any point in time.

Measures for ensuring physical security of locations at which personal data are processed

- All data processing occurs at AWS data centers. Specific physical controls are not disclosed by Amazon however they have provided verifications of physical security via independent audit to

us and we have provided that information to our audit team. We are unable to disclose that information publicly due to non-disclosure requirements.

Measures for ensuring events logging

- Every interaction with the Groupize application is automatically logged to the Salesforce Heroku log feed. That feed is then aggregated via Papertail, a log management and search utility.
- Logs are kept in an interactive state for 1 month.
- Logs are kept in an archive format for 1 year

Measures for ensuring system configuration, including default configuration

- Salesforce Heroku defines the standards by which Groupize application servers are configured. This includes a secure and hardened system configuration on dedicated instances.

Measures for internal IT and IT security governance and management

- Groupize maintains a full Information Security Management System (ISMS) which is annually audited for compliance with the ISO/IEC 27001:2003 standard.
- This program is reviewed, at least, annually by executive management for compliance with stated organizational objectives and any necessary changes.

Measures for certification/assurance of processes and products

- The Groupize application is audited annually for PCI DSS compliance by Security Metrics
- Groupize as an organization, and the Groupize application, are audited annually by Aprio for ISO/IEC 27001:2003 compliance.

Measures for ensuring data minimisation

- Groupize maintains a data retention policy that outlines what data is kept and for how long. Depending on the context of the data it may be anonymized in part prior to full deletion at a later date.
- By default events are configured to only request basic personal information from participants (notably name and email address). Planners may, at their discretion, enable additional fields. Planners are advised in app, and during training, to only request the information that is necessary to achieve the objectives of their event.
- Planners may, at their discretion, purge event data via manual deletion processes available in the application.

Measures for ensuring data quality

- All data is validated for accuracy as it is entered, depending on the context. Validation might include a requirement that data be provided, checking for the format of the data, and security-level validations such as ensuring data cannot trigger an XSS or SQL Injection attack.
- Validation rules are, at times, defined by the event planner who can choose specific types of fields and if a field is required or optional for registration.

Measures for ensuring limited data retention

- Groupize maintains a data retention policy that outlines what data is kept and for how long. Depending on the context of the data it may be anonymized in part prior to full deletion at a later date.
- Deletion of data within the application is via automated process or manual customer request as needed.
- At any point a customer or user can put in a support ticket, or contact support@groupize.com, to request the removal of data.

Measures for ensuring accountability

- Work products are regularly peer reviewed, especially application changes which require a peer code review before they can be elevated to a hosted environment.
- Annual employee reviews ensure that individuals are maintaining an expected and necessary level of competence in their roles.
- Groupize maintains a full disciplinary policy in the event that a violation of policy, including information security policy, should occur. The disciplinary policy outlines the possible consequences of such a breach which vary from reprimand to termination depending on severity.

Measures for allowing data portability and ensuring erasure

- Functionality exists within the Groupize application to allow a planner to export attendee or event information which would allow that data to be migrated to another system or use case as needed.
- Should a registrant need to export their registration data they would be directed to email support@groupize.com where Groupize customer success could prepare an export on their behalf, while excluding any other registrant data. The attendee could also address that request to the event planner for their event.