Privacy, security and Architecture of Repcamp (Includes web based app and Android, iOS app)

One of the Repcamp's main objectives is to maintain the security and privacy of our customers. In order to achieve this goal, Repcamp provides a robust security and privacy program that covers personal data protection and data submitted by customers to our cloud software ("Customer Data").

This documentation describes the architecture and the administrative, technical and physical controls applicable to our software branded as Repcamp.

Software Architecture and Data Segregation

Repcamp Software is operated in a multitenant architecture that is designed to segregate and restrict Customer Data access. The architecture provides an effective logical data separation for different customers via customer-specific "Organization Gids" and allows the use of customer and user role-based access privileges.

Control of Processing

Repcamp has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by Repcamp and its subprocessors.

Third-Party Functionality

Certain features of the Software use functionality provided by third parties. Although we never transmit customer data to such third party without a previous authorization.

Audits and Certifications

The software undergoes security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis.

Security Controls

The software includes a variety of security controls that allow customers to tailor the security of the software for their own use.

Security Policies and Procedures

- Customer passwords are stored using a one-way salted hash.
- User access log entries will be maintained, containing date, time, user ID, URL executed or entity ID operated on, operation performed (created, updated, deleted) .
- If there is a suspicion of inappropriate access, Repcamp can provide customers log entry records and/or analysis of such records to assist in forensic analysis when available. This service will be provided to customers on a time and materials basis.
- The software maintains in Amazon S3 service logs, system infrastructure logs, and application logs.
- Passwords are not logged.
- Repcamp staff will not set a defined password for a user.

Intrusion Detection

Repcamp, or an authorized third party, will monitor the software for unauthorized intrusions using network-based and/or host-based intrusion detection mechanisms. Repcamp may analyze data collected by users' web browsers for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the Covered Services function properly.

Incident Management

Repcamp maintains security incident management policies and procedures. Repcamp notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by Repcamp or its agents of which Repcamp becomes aware to the extent permitted by law.

Repcamp publishes system status information on the Repcamp website. Repcamp typically notifies customers of significant system incidents by email.

User Authentication

Access to the software requires authentication using user ID/password. Following successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

Physical Security

Our software is completely hosted in the Amazon AWS infrastructure. For more information about AWS security systems in relation to GRPD visit [All AWS Services GDPR ready | AWS Security Blog]

Reliability and Backup

Our web servers hosted in AWS are configured in a redundant configuration. All Customer Data submitted to the software is stored on a NoSQL database and the Data is periodically replicated to S3 Amazon Service. Backups are verified for integrity and stored in S3.

Disaster Recovery

The Repcamp's disaster recovery plans currently have the following objectives:

(a) restoration of the service within 12 hours after Repcamp's declaration of a disaster.

(b) Maximum Customer Data loss (recovery point objective) of 4 hours.

However, these targets exclude a disaster related to our hosting provider (Amazon AWS) causing the compromise of our service.

Viruses

The Software do not scan for viruses that could be included in attachments or other Customer Data uploaded into the software platform by a customer. Uploaded attachments, however, are not executed in the platform and therefore will not damage or compromise the platform by containing a virus.

Return and deletion of Customer Data

Within 30 days post contract termination, customers may request return of their respective Customer Data submitted to the Covered Services (to the extent such data has not been deleted by Customer).

Repcamp shall provide such Customer Data via a downloadable file in comma separated value (.csv) format and attachments in their native format.

After termination of all subscriptions, Customer Data submitted to the Covered Services is retained in inactive status within the Software for 30 days, after which it is securely overwritten or deleted from production within 90 days.

Analytics

Repcamp may track and analyze the usage of the Software for purposes of security and helping Repcamp improve the Software. However, Repcamp will never use customer personal data for any purpose without its authorization.

Transactional messages

Repcamp may contact users to provide transactional information about the Software. Repcamp offers customers and users the ability to deactivate or opt out of receiving such messages.