CustomerGauge Information Security Plan

Information Security Plan
v2.13 29/07/20

Adam Dorrell
Antony Laycock
CustomerGauge
EUROPE: Van Diemenstraat 182B, 1013CP
Amsterdam, NL
USA: 3 Burlington Woods Burlington 01803, MA

Table of Contents

Document Change History

- v1.0 September 12 2014: Created
- v1.1 April 7 2015. Added privacy policy and Business Continuity plan
- v1.2 Jan 7 2016. Added Disaster Recovery Plan
- v1.3 Feb 9 2017: Reviewed by AL/AD, Added additional details on changes to APIs, upgraded security items on AWS, updated links
- v1.31 Feb 13 2017: Updated links - made most public

- v1.4 Refresh Based on RFP FAQ
- v1.41 Format refresh following move to Confluence
- v1.42 Added some information based on RFP experience. Attached AWS DPA / Sendgrid Model Clause.
- v1.43 13 April 2018 Minor Edits
- v2.00 Updated to reflect GDPR compliance. De-duplicated information between Privacy Policy, SLA, Terms of Service and DPA
- v2.10 29/04/19 Yearly Review Updates
- v2.11 09/05/19 Update following May Infosec Team Meeting
- v2.12 02/03/20 General Refresh - Hardening and Cognito now mentioned.
- v2.13 29/07/20 A few extra clarifications based on common questions and recent improvements

1. Introduction

This document describes the technical and organisational measures that are in place to ensure CustomerGauge fulfills its role as a GDPR compliant Data Processor.

- To understand what data CustomerGauge captures (from our websites and product) and how we use it, please see our **Privacy Policy** here: https://customergauge.com/privacy-policy/
- To read or **Service Level Agreement** which includes our **Business Continuity Plan** see here: https://support.customergauge.com/support/solutions/articles/5000789667-customergauge-service-level-agreement
- For our **Terms of Service or Data Processing Agreement** contact Customer Support

2. Incident Response Plan (IRP)

This document explains the measures we take to ensure your data is protected from illegitimate use. In the unlikely event that these measure prove insufficient we will follow an incident Response plan based on the standards in the "Computer Security Incident Handling Guide - Recommendations of the National Institute of Standards and Technology" https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

If you want to report a data security incident

Your Customer Success Team representative is your first point of contact for any data security concerns. From there, the standard escalation path (dependent on severity) is:

- Customer Success Team
- Technical Team
- Head of Tech
- CustomerGauge management team
- CEO (available in 4 hours 24x7) for Severity 1

If CustomerGauge detects a high priority data security incident e.g. breach.

We understand that our Customers, as Data Controllers, have a GDPR obligation to report data breaches to authorities and affected data subjects within 72 hours. As Data Processors, CustomerGauge will support this obligation. (

With respect to monitoring, we use a DevOps partner (see Suppliers Section) to help manage our AWS account. They have a comprehensive set of alarms, including those that trigger on high levels of suspicious access activity. In addition, the CustomerGauge technical team makes daily use of 'Kibana' application logs.

In case of a suspected breach, the process will be :

- Member of CustomerGauge staff that suspects potential data problems will raise an internal ticket for the Tech Team to investigate.
- If confirmed the Head of Tech Department (or a deputy) will prepare an 'Incident Report' for the CustomerGauge Management Team.
    - Example of the internal **CustomerGauge Security Incident Response Form**.

- The Management Team will review the report and if the incident is confirmed will analyse the extent and impact. Customer communication will be prepared and it will include the information required by GDPR breach reporting rules:
    - describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
    - communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
    - describe the likely consequences of the personal data breach;
    - describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Customers will be informed within a maximum of 24 hours of this information becoming available.

Data Incidents that do not involve a breach.

e.g. A system or hardware defect causes data pollution or deletion. This will normally be dealt with internally as our comprehensive backup system will facilitate a restore operation. However, if this was not sufficient to completely resolve the problem then the incident reporting process will be:

- Member of CustomerGauge staff that suspects potential data problems will raise an internal ticket for the Tech Team to investigate.
- If confirmed the Head of Tech Department (or a deputy) will prepare an 'Incident Report'.
- Affected Customers will be informed via Customer Success Department, or in severe cases, by CEO.

Request from authorised lawful entity for Data on individual.

COO will validate credentials of the requester before approving.

Other Scenarios
Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies). These are handled through CEO and COO on ad-hoc basis
Management Team are notified weekly of any items.

3. Data Access Control

Correctly handling our clients data is essential. Clients trust us to hold valuable data on their behalf. We need to comply with relevant laws as a minimum, but take all precautions to ensure that we handle data with the greatest of care.

Definitions:
• “Data”: all the information that is given to us by our Clients (by upload), and their
Customers (by survey), and derived results of this processing.
• “Sensitive Information” – any information that can personally identify an individual such as email, name, telephone.

We employ several layers of data security:

• Electronic – access control to systems

- The CustomerGauge platform itself
- Other systems that can access (partial) data captured by CustomerGauge platform.

• Processes for employees

- when data should be accessed
- how data should be accessed
- permission management and revoking access

• Physical – access to systems with data on

- Office Locations
- Server Locations

For detail, see the following sections.

3.1 Access to CustomerGauge platform

User Provisioning & Authentication

- Users are created by Customer Admin users.
- Users' username & email are the only mandatory fields.
- The authentication process is based on a traditional username/password combination.
- Passwords are hashed and salted using SHA-256
- User Password Policy **REQUIREMENTS**
  - Special Character (except: @, #)
  - SmallCap Character
  - Cap Character
  - Number
  - More than 8 characters
  - No sequential numbers
  - No username, last name or company
- The system is locked after five failed access attempts. Sys admin intervention is required to unlock the system.
- User Credentials are stored encrypted in 'AWS Cognito' User Management service which provides secure password reset option.
  - So CustomerGauge Employees should never be aware of Users' Passwords
- There is not currently an option for direct use of MFA on CG platform, though SSO from systems that do support MFA is possible.

Session Management

Sessions are managed automatically from our PHP framework and stored into a redis database. The redis database is only accessible from within AWS or via Bastion host and whitelisted IPs.

CG has an automatic session expiration having an Idle Timeout set at 2 hours and an Absolute Timeout set at 1 day.

IP Restrictions

The CG platform offers the possibility to restrict the access to a trusted list of IP addresses. Admin users will find a module "Security" in the admin menu and they are able to enable/disable the feature providing a list of IP addresses.

Enabling the feature the system will perform an additional check during the authentication process and deny the access in case the client's IP does not match with the whitelist. Whitelists can control:

- User Access to the CG platform
- Programmatic Access to the APIs
- Visibility of the 'Digisign' Slideshow Report

User Access

CG stores the following information about User Access and Logins.

- User last login date
- User last password change date
- User last password reset date
- User last wrong login attempt date
- User login count
- User wrong attempts count

However this information is not available from within the CG tool. Instead a client admin can request for this information via our helpdesk, specifying the reason why it is requested. The information will be delivered by CSV file.

CG ADMIN User Actions

Our CSM team at CG can make major changes to the system configuration. We hold Audit logs of the step-by-step changes in case we need to diagnose issues or roll-back to previous state. e.g. Segment Editing, Mail Rule configuration.

CG Employees can only access the CG Internal Admin Tool via GSuite SSO.

Customer ADMIN User Actions

Customer Admin Role can make major changes to the system configuration. We hold Audit logs of most of the step-by-step changes in case we need to diagnose issues or roll-back to previous state. e.g. Changes to User Permissions, Upload Field mappings, IP Whitelisting

3.2 Employee access to Customer Data

Permission and Policy

CustomerGauge employees must adhere to a policy of not accessing customer data unless by direct delegation in case of urgent tasks or specific maintenance requests from customers. This process is managed and audited via our ticketing systems.

When permission to access data is given, via a ticket being raised to investigate a problem, the Employee will access the CustomerGauge platform in the same way as a regular admin user, but with a dedicated CG-Support or CG-Tech username.

This is important as CustomerGauge operates a 'clean desk' policy i.e. Customer Data should not be transferred to employee laptops or printed out. If, in the course of handling a maintenance request, it was essential to transfer customer data to laptop, say via export function, then this data must be removed by end of business, same day, at the latest. Data should never be transferred by physical media.

If a copy of some data needs to be logged on the internal or external ticketing system (e.g. as a screenshot) then personal data must be obfuscated.

3rd Party Access

CustomerGauge uses the services of a 3rd party DevOps provider(s). Our policy is that the 3rd party may have access to the server systems but not the data they contain. Copies of the partner's Security Policies are available on request.

This partner also has access to the CustomerGauge codebase in order to help diagnose any out of hours problems though, in general, Customer Gauge does not outsource any code development.

CustomerGauge takes responsibility that our Partners comply with the standards described here. We retain the right to change suppliers if necessary, though new Suppliers would be bound by at least the same security requirements.

Education & Security Awareness

Regular 'all-hands' training sessions are held by our CEO (or Deputy). All new starters + 6 monthly refreshers. This covers regulatory changes (e.g. introduction of GDPR), clean machine best practices and general safety measures on the open internet etc.

CG Internal Password Management

Passwords must be memorized or stored in the corporate account of a Cloud Based password management tool (currently 1Password).

Browser password management must be disabled or protected by a master password.

It is mandatory to use strong password rules.

- Laptops
- CSM & Tech logins to CG platform
- Logins to business critical applications

Employee Access to Data

It is occasionally necessary for employees to continue problem investigations by accessing the relational Database directly. Again, this must be covered by a request in the ticket system. Database logins are personal and granted with limited permissions based on role.

Access is via db username & strong password and possibly MFA depending on connection method.

Furthermore all production database are protected by a VPC and accessed by an IP locked Bastion server. They can be accessed only from within the VPC, our offices or from approved employee home addresses.

Database connections are SSL secured.

Secondary Uses of Customer Data

CustomerGauge will not pass on customer data to any third parties except for operational purposes (partners listed explicitly in this document). We have DPAs in place that these partners will not access customer data.

However, CustomerGauge does make use of the data sets in order to improve system performance and to provide industry benchmarks, *in such a case, the data will be fully anonymised.*

3.3 Revoking Access / Data Deletion

Employee Leaver Process

A formal leaver process is in place. It includes a checklist of system access points. Access is removed on completion of the employee's final day with the company. At this point we also check the access lists for unexpected entries.

Physical Deletion of Customer Data on Service Termination

In case of service termination CG will permanently delete the full client database within one month of contract ending or sooner if explicitly requested. Database daily and incremental Backups will be deleted automatically within one month of database deletion.

We provide a Certificate of Destruction on request. Request Procedure and Certificate of Data Deletion for details.

GDPR right to revoke permission

CG platform does not store highly sensitive data such as credit card or national id numbers by default. However, it is possible for customers to choose to load sensitive date in our 'User defined fields'.

To comply with GDPR we have an 'anonymise' API available that will replace personal data with '****'. This anonymise process will include User Defined Fields where 'Personal Data' has been indicated.

Employee Devices

There is an Asset Management process in place that ensures storage media (including laptops) is destroyed or hard erased at end of life.

3.4 Physical Access Restrictions

Office Locations

CustomerGauge has a self-contained office space and do not have a shared entrance with other organisations.
• In our office spaces, office, CustomerGauge employs an access control system that records the time of entry and exit of individual employees (or contractors). Records are kept for 90 days.

Office Network Security
• Client services and others have access to wifi. There are separate Guest and Internal networks, secured by password.
• Firewall rules are enabled on the Cisco RV042 router to prevent unauthorised access. Open ports have been blocked. Remote configuration is blocked.
• Virus protection is kept up to date on Windows systems.

CustomerGauge policy is to provide corporate devices for all employees. Use of personal devices for corporate purposes is in exceptional cases only and requires approval.

• Physical access is restricted to employees and contractors. Where other individuals need access, they must be accompanied for the duration of the visit.

Server Locations

The CustomerGauge platform is hosted entirely in AWS.

All employees that require access to the AWS console must enable Multi-Factor Authentication.

Separation of AWS Accounts

We use several AWS accounts in order to provide 'least privilege' role based access rules. (Production, DTA, Shared Services, Billing, User Access Management, Research.)

4. Technical Data Security

4.1 Multi-Tenancy and Data Segregation

We have a separate database per customer in each RDS system. No RDS tables containing private data are shared with other customers. Each Tenant's Database is associated to a specific MySQL user in order to ensure the maximum of the security.

4.2 Data at Rest

Data is encrypted at RDS server level based on AES256. We use a an AWS Managed Database service and AWS manages the encryption keys.

4.3 Data in Transit

Data in transit between the tool and clients are always secured by TLS1+. Key size asymmetric 2048 bits
Data in transit from SFTP are secured by an SSH tunnel and protected by a DSA / RSA 2048 bit private key

4.4 Third Party SaaS Suppliers

AWS

AWS is used for all application hosting. We use the following AWS Regions:

- EU - Ireland
- AU - Australia
- US - North Virginia

Region is selected by the customer during onboarding. No data is transferred outside of this region unless explicitly requested by the customer.

CustomerGauge has a DPA in place with AWS Ireland. AWS_Data_Processing_Addendum__DPA___Self-Service___2016-12-12_CG8March2017.pdf

Sendgrid

Sendgrid is a market leading Email SaaS provider. They are based in the US and of course they distribute mail globally, but we have a model clause in place with them SendGrid_EU_Model_Clauses.pdf

Nexmo

Nexmo is a market leading SMS SaaS provider. They are based in the US and of course they distribute SMS globally. Their terms and conditions are GDPR compliant. DPA is in place.

CloudElements

CloudElements is a Saas provider that simplifies integrations with CRM & ERP systems such as Salesforce & NetSuite. It is also GDPR compliant and covered by Privacy Shield.

Oblivion b.v.

Is an Operations partner and AWS Consultancy that help CustomerGauge provide 24/7 cloud incident coverage. A DPA is in place.

4.5 Backup schedule

This section relates to customer data that is stored on the CG platform.

- Back-ups are fully automated and managed by AWS RDS and are stored in the same Region.
- It makes a daily full-backup which takes place at 4:00 AM (UTC). This process generates a full snapshot and it gets stored into a different AWS availability zone in the same region.
- Furthermore it makes a point-in-time recovery with a 60 minutes increment.
- Backups are encrypted using AES-256.
- The time required for restoring a backup could depend on the size of the DB itself. For our experience it would not take more than 4 hours.
- Backups are automatically purged after one month.

4.6 System and Network Security

CG fully relies on Amazon Web Services cloud infrastructure. As company leader on cloud computing it offers the most advanced certifications and it complies with most important standards on network security and IT management as ISO27001, ISO9001, SOC1-2-3.
Our account's servers are configured to only open ports specifically required for the application to function.

https://aws.amazon.com/compliance/data-center/controls/

AWS Shield is enabled to combat DDoS attacks.

The core components of the CustomerGauge architecture are running in a dedicated VPC (Virtual Private Cloud).

Cross account communication is facilitated by dedicated NAT and Bastion servers.

Our VPC setup acts as a Network Firewall but we do not currently have a Web Application Firewall (WAF) in place.

5. Technical Architecture

CustomerGauge provides its service through a Software as a Service model based on a microservices architecture where components are auto-scaled & auto-healed using AWS Cloudwatch availability alerts. Core services are running in Docker Containers on ECS using Fargate clusters. Inter-service communication is provided via queues (SQS) for extra resilience.

5.1 Operating System Patches and updates

Our 'Serverless' approach (i.e. Using Lambda or Fargate) means that AWS is responsible for providing hardware with suitably patched Operating System.

Our Docker containers are built using automatic deployment pipelines and so dependent packages can have versions updated as necessary with each major or minor software release, so possibly every two weeks.

Production Environment is 'Hardened' compared to Test Environments. This means Operating System and Library dependencies are stripped down to the bare minimum needed to run the application. We make extensive use of 'Alpine' as our Docker base image. Our build process includes scanning for vulnerable versions of imported dependencies using 'Dependabot'.

5.2 Deployment Schedule

Our deployment schedule is normally bi-weekly as a result of our Agile development methods. Each release can be rolled back if needed. A list of deployments is posted here: CustomerGauge Release Notes: {+}https://support.customergauge.com/support/solutions/folders/5000282839+

5.3 Malware

Our core services are Dockerized / Serverless and the virtual machine instances they run on are managed by Amazon and recycled on a daily basis, there is therefore a low risk of malware infection.

5.4 Debug Logging

Debug logs contain the minimum amount of customer's personal data required to support system diagnostics. Access is restricted to Developers only and is IP locked. Logs are automatically deleted after a set time period, currently 90d.

6. Development Standards

6.1 SDLC

CustomerGauge follows an Agile development process (currently Scrum). Each new User Story is analysed, designed and tested taking into account a jira maintained list of ongoing Non-Functional Requirements, including data security requirements. The team maintains a list of 'Defensive coding standards' that are in scope for all stories.

6.2 Secure Coding practices

80% of our back-end code is based on PHP, 20% based on Python and NodeJS.
As best coding practices we follow the OWASP Secure Coding Practices and we include the following check-list within our development cycles. The check list is divided in *General Coding Practices, Input Validation, Output encoding, Authentication, Session Management, Error Handling, System Configurations, Database Security, File Management, Memory Management.*

6.3 Vulnerability Fix / Remediation Process

The development team follows an Agile development process (Scrum). Vulnerability fixes are raised as high priority user stories, or bugs, and addressed in the current, or forthcoming, sprint dependent on priority.

6.4 Testing

Testing at CustomerGauge is divided into a number of areas:

- Automated Unit Testing - Unit Testing is embedded into our development cycle. All code developed since ~ 2017 will average 100% coverage, though it is possible some older code has less coverage.
- Application Security Testing - Each major release is tested using industry standard scanners (e.g. BURP suite) to check for newly introduced vulnerabilities.
- 3rd party penetration tests are performed roughly yearly. Report can be shared on request.
- Manual Testing - As an addition to our strict Unit Testing we also run manual tests as part of the development cycle. We run several manual tests and usability tests on 4 different environments: Local machine, development environment, QA environment and final production environment. If any errors are found we proactively work in order to fix issues having a bug-free environment before a push to production.

During our product/feature planning workflow we do also integrate a checklist we should perform for each testing round across all environments.

Any potential security vulnerabilities detected are entered into our defect tracker system (Jira) as Critical or Major priority bugs. The outstanding bug list is displayed on an organization wide dashboard.

Customer Data is never used in Test Environments, unless fully anonymised.

6.5 Source Code & Change Management

The Development Team uses JIRA to track bugfixes and features. All software releases are explicitly mapped to the issues they contain.
The Development Team uses GitHub as a source control system. We maintain the following branches:

- Feature Branches : Used for work-in-progress for a single developer or a small group of developers. We advocate that these branches are short lived so as not to delay integration attempts.
- DEV Branch : Used for integrating work-in-progress of the team as a whole.
- QA Branch : Used for acceptance testing features that are candidates for release.
- Master Branch : Represents the Production version of the code.

All releases are tagged such that failed deployments can be rolled back to previous version. Such a roll-back can be achieved within around 30 minutes. GitHub repositories are private and access is role based.

All newly written code is peer reviewed prior to being merged.

6.6 Infrastructure as Code

Cloud resources are created and configured using 'Cloud Formation' scripts. These scripts are subject to the same Development process described above.

Certifications

CustomerGauge platform is designed to operate on the lowest grades of personal data (e.g. email only) so the many Financial and Medical Data Protection Certificates are out of scope.

We are GDPR compliant and we encourage our development staff to become AWS Associate level certified.

Our physical data centres are extensively covered by various compliance bodies. https://aws.amazon.com/compliance/

7. Business Continuity Plan (BCP)

In addition to protecting our customers' data we will also protect our customers' access to that data by providing a comprehensive continuity of service plan.

7.1 Office Location Issues

Eg. fire at office, power outages, loss of internet, theft of computers, etc.

Effect is minimal as the Saas platform itself and all key IT systems are hosted in the cloud and can be accessed via a browser from any suitable device (e.g. : Email (general communication and support etc), Support ticket system, Billing system, Phone system (VoIP), CRM system (Salesforce). In fact many staff members already work remotely on occasion, with IP whitelisting for extra security.

Although the organization can function in 'WFH' mode effectively, we do also have a 'warm office' alternative for our Amsterdam HQ in Van Diemenstraat. Lauriergracht 91, Amsterdam, is approximately 3km away and is fully equipped with alternate internet, power, light, heat, and space for at least 8 key workers. This is ready to go 24x7

In case of temporary power outage all workers have laptops and can continue for several hours on batteries.

7.2 Server Location Issues

The CustomerGauge platform is entirely hosted in Amazon datacenters.

In the event of a planned or unplanned outage server or RDS outage All core systems will automatically switches to a standby replica in another Availability Zone. (An AWS 'AZ' is one or more data centres, within a region, that are geographically separated from other data centres within the same region. The separation needs to be far enough to such that a natural disaster could only affect a single AZ. Hence the majority of failures will not impact availability.)

The failover of RDS across Zones is regularly tested as we rely on this feature to retain system availability during RDS maintenance windows (twice a year on average).

There is no transfer or replication of data across AWS Regions.

In the case of accidental data deletion through employee error or software malfunction, databases can be restored on a per customer basis with increments of one hour.

7.3 HR issues

All senior staff have a designated backup, and in the event of illness, injury or other event that would incapacitate a staff member, responsibilities would transfer to the alternate. This is used regularly in vacation cover.

Follow-the-sun support can be provided by our offices in Amsterdam, Boston and Sydney, so at any time it is possible to get advice and support from CustomerGauge. There is an internal DPA to ensure GDPR obligations are covered in case of cross region data access.