Client notification Messaging and Voice

26-07-2021

This document belongs to:
CM.com Netherlands B.V.
Konijnenberg 24
4825 BD Breda
Tel: +31 76 572 70 00
E-Mail: info@cm.nl

Classification: Public

Revision	Change details	Release date
V0.1	Initial version.	26-04-2021
V0.2	Minor changes	30-04-2021
V0.3	Minor changes	16-07-2021
V0.4	Minor changes	23-07-2021
V1.0	Updated version	26-07-2021

Client notification Messaging and Voice

CM.com fulfills the role of Cloud Service Provider (hereafter: CSP) when you are accessing the services that CM.com offers. Cloud Service Customers (hereafter: CSC) do not have direct access to CM.com's CSP infrastructure.

CM.com's information security framework is based on the ISO27001 Information Security Management System. This has been extended by additional controls of ISO27017 and ISO27018.

This includes, but is not limited to:

- Access Management;
- Asset Management;
- Business Continuity Security;
- Cloud Infrastructure Security;
- Communications Security;
- Cryptography;
- Incident Response;
    - Data breach;
- Network Infrastructure Security;
- People Security;
- Physical Security;
- Product Security;
- Security Compliance;
- Security Monitoring;
- Capacity Monitoring;
- Vulnerability Management;
- Clock synchronization;
- Platform availability;
- Backup;
- Data storage;
- Data retention;
- Data deletion;
    - Data retention after termination of the contract;
- Processors & Sub-processors;
    - Processors;
    - Sub-processors;
- Laws and regulations.

All CSP services of Messaging and Voice are hosted on CM.com privately owned and operated cloud environments. CM.com has full control over all data, including its transport, encryption and accessibility.

There are no third-party cloud services involved in the creation, hosting and delivery of our services.

'Personal data' can also be read as 'Personally Identifiable Information (PII)'.

Access Management

CM.com has taken different measures to:

- Ensure protection of the information systems from intrusion;
- Protect data from unauthorized alteration and corruption;
- Protect the supporting infrastructure from disruption and to prevent unauthorized access.

Asset Management

CM.com ensures the registration and classification of all relevant IT/information assets. This includes information about the lifecycle factors of these assets in relation with the classification level. These factors are: creation, secure processing, storage, transmission, deletion and destruction.

Business Continuity Security

CM.com's main goal is to deliver a global platform with all channels and features to best communicate with your audience worldwide. Our Communications Platform as a Service (CPaaS) contains all Messaging and Voice channels, as well as next gen payments and smart identification tools. And with our customer data platform (CDP), we provide you an easy use of these features.

We aim to be flexible, scalable and fast at delivering the services to our customers, while maintaining the highest standards in security and compliance. The platform runs on own and self-operated servers and software. It is hosted in our own datacenters and in external datacenter locations of top-tier certified suppliers.

Measures are in place to monitor, control and continuously improve data security and business continuity.

Cloud Infrastructure Security

The cloud infrastructure is hardened according to best practices and security guides based on input from organizations such as CIS and NIST.

Communications Security

CM.com defines policies, procedures and agreements to mitigate the risks with respect to confidentiality, integrity and availability. The risks regarding these topics are also addressed in CM.com's risk and control register.

CM.com has a strict internal confidentiality policy. All employees are trained in this at onboarding and on an ongoing basis. Agreements are defined in each employment contract.

Cryptography

CM.com has taken different measures to ensure a correct and appropriate use of cryptographic controls to protect the confidentiality, authenticity and integrity of data. CM.com adheres to the applicable laws and regulations per country where CM.com is located.

Incident Response

In case of an information security incident, CM.com has an incident response plan, including the following protocols to respond adequately:

- Security team is available and together with the support team, the security team provides 1st, 2nd and 3rd line support and response in case of incidents;
- A business continuity plan to eliminate the threat, contain the damage, restore service availability and implement structural remedies to prevent repetitive incurrence;
- In the event of a security incident, we inform customers via appropriate communication channels such as https://status.cm.com, e-mail or a personal phone call, depending on the severity and SLA-levels.

As an electronic communications provider, CM.com has an independent duty to inform the respective authorities in the case of security incidents and/or network disruptions.

Data breach

In respect of a personal data breach, CM.com notifies each affected client of a personal data breach involving CM.com or a sub-contractor without undue delay (but in no event later than forty-eight hours after becoming aware of the personal data breach). The notification will be communicated via e-mail to the relevant contact persons.

Network Infrastructure Security

Network components, such as firewalls, routers and switches are always protected with named accounts and therefore strong password policies are in place. Logical access to diagnostic and configuration ports is restricted to a selected group of employees and is only accessible via selected terminals. The same applies for the physical access to diagnostic and configuration ports; only a few employees have physical access to these devices.

People Security

CM.com secures personnel integrity through background verification checks, contractual conditions and regular awareness trainings.

Physical Security

To prevent unauthorized physical access, damage, and interference to CM.com services, used premises and information processing facilities, CM.com has taken different measures to ensure the physical security and access to those facilities.

Product Security

Every product is delivered according to secure coding best practices. Additionally, vulnerability scanning is executed periodically.

Secure Software Development tooling like SAST/DAST/RASP (or a combination) are used to review the code for vulnerabilities as well.

Security Compliance

The primary responsibility for compliance is with the operational business management. The Legal department informs the organization of relevant laws and regulations and implement the relevant procedures to ensure compliance. Furthermore, in a more general way, the Legal department, supported by other relevant functions, raises awareness in the organization with regards to applicable legislation that applies to various business processes. Relevant legislation and regulations have been translated in our internal compliance framework.

Security Monitoring
The SOC department is responsible for monitoring of the entire CPaaS platform 24/7/365.

Capacity Monitoring
CM.com is responsible for monitoring and reporting of the operational components and the performance of the cloud infrastructure. This ensures that sufficient capacity is available at all times in order to meet the agreed capacity and performance-related requirements in a cost-effective and timely manner.

Vulnerability Management
In order to facilitate a safe working environment, the usage of workspaces, devices, tools and software provided by CM.com is bound to specific guidelines. Several lines of defense are in place:

1. Education of users;
2. Endpoint protection;
3. Semi-automated patching of all systems in scope;
4. Advanced mail protection;
5. Monitoring of systems and servers behavior on the network;
6. Firewalling including next-gen features.

Clock synchronization
Clock synchronization is done by using global publicly available NTP-servers. The cloud platform synchronizes the clock by connecting to pool.ntp.org or to a specific NTP-region when needed. CSC can use pool.ntp.org. The system will try finding the closest available server.

Additional information can be found on: https://www.pool.ntp.org

Platform availability
The CSC is able to monitor the platform status (via: https://status.cm.com).
The CSC can leverage below options to monitor the availability of the CM.com platform:

- For Voice: SIP “OPTIONS” Message;
- For Messaging: API health check on port TCP 443.

Further information can be obtained by contacting support@cm.com .

Backup
Backup of the environment is the responsibility of the CSP. Backups are encrypted in transit and at rest (AES256 – Advanced Encryption Standard). All components in order to guarantee business continuity, such as configuration data, user data and message data are being backed up. Automated ‘snapshots’ are taken daily. Backed up data is retained redundantly across two availability zones.

Integrity of backups is verified using file fingerprinting. Backups are restored periodically in an automated way to an isolated test environment where the data is anonymized and used for restore validation. Recovery Time Objective (RTO) is set in order to guarantee business continuity and availability.

Data storage
CSC data at rest (and data residing in backups) is stored in the EU (The Netherlands) on CM.com’s privately owned (and managed) public cloud environment.

Data retention

Personal data is retained by CM.com for a limited period. This 'retention period' may vary per service and per data type. All retention periods are compliant with the relevant and applicable telecom & data protection legislation and guidance from national authorities and operators. In principle all personal data is stored no longer than strictly required.

Data deletion

Removal of personal data is done on production systems and personal data will be present in the backups for a limited period. This data is automatically anonymized after the retention period of the backup has lapsed.

Data retention after termination of the contract

After termination of the contract, data including personal data will be present in the production system for the periods specified below:

- Client data: twelve months;
- Voice: six months;
- Messaging: eleven months.

After these periods, the data will only be present in the backups which have a retention of three months. This data is automatically anonymized after the retention period of the backup has lapsed.

Processors & Sub-processors

CM.com may process personal data either as a data controller or as a data processor. Personal data may include Client Personal Data and End-user Personal Data.

Processors

Personal Data of (the employees of) Client is or may be collected by CM at the time of registration and/or during the performance of this Agreement. Where CM.com is processing Client Personal Data they shall act as a data controller under applicable Data Protection Laws. Other data concerning the Client may include contact data, financial data and Platform usage data. Any such data is processed for contract management purposes, customer support, credit checks, prevention of fraud and criminal activities and 'know your customer'('KYC') processes.

In providing our services we use applications and services of our trusted suppliers. These suppliers may process Client Personal Data on our behalf. The processors are listed below.

Processor	Location	Purpose	Transfer Mechanism
Salesforce SFDC Ireland Limited.	Ireland (EU)	Provision of CRM Platform	DPA and Binding Corporate Rules
CM.com affiliates in Netherlands	The Netherlands	Support, contract management, provision of services	CM.com Internal DPA

Sub-processors

Other than CM.com affiliates, CM.com does not use sub-processors for providing the Messaging and Voice services, noting that providers of electronic communication services with whom CM.com is contracted, are not considered sub-processors. The service offered by CM.com is the delivery of the traffic to the telecom operator of the end user. The telecom operator is a controller in the relation to the end user. CM.com itself, offering such services will be considered a controller in respect of the processing of the personal data necessary for the operation of the service (i.e. traffic data). The providers of telecommunications services are considered controller for traffic and billing data.

Processor	Location	Purpose	Transfer Mechanism
CM.com Affiliates in the Netherlands	The Netherlands (EU)	Support, contract management, provision of services	CM.com Internal DPA

Law and regulations

CM.com has the required licenses and registration to offer the service in the countries where it is located, and has the required policies and procedures to ensure continuous compliance with applicable law, regulations and operator guidelines.