Information Security Practices

Cegid SaaS

Cegid SaaS - Information Security Practices

CONTENTS

1. Document versions

Version	Release Date
PAS_CEGID_SAAS_V2016-07_EN	August 3, 2016

2. Introduction

2.1. Purpose

The Cegid SaaS Security Practises enables to describe the commitments taken by Cegid in terms of information security for the SaaS services it operates.

2.2. Scope

This document applies to SaaS services operated by the SaaS Cegid Production department.

This document applies to Cegid SaaS activities operated on data centers located in France (Cegid private cloud / IBM and Cegid control center).

2.3. Definitions

Assets: Goods or services needed to provide Cegid SaaS services

IPS: Intrusion Prevention System

Terms of Service: Document describing the specific conditions related to each Cegid SaaS service

SaaS Production: Organization within Cegid in charge of the design, operation and technical support of Cegid SaaS platform (cf. Presentation of the SaaS Production department)

ISSP: Information Systems Security Policy

RPO: Recovery Point Objective

CISO: Chief information security officer

RTO: Recovery Time Objective

ISMS: Information security management system. This term refers to a set of policies related to the management of information security

VPN: Virtual Private Network

2.4. References

ISO 27001: Standard requirements for Information Security Management Systems (ISMS)

ISO 27002: Guide to ISMS best practice.

ISO 27005: Standard for the management of risks related to information security

Terms of Service: Documents describing the specific conditions related to each Cegid SaaS service. They are available on Cegid's website, www.cegid.com

SSA: Subscription Services Agreement. They are available on Cegid's website, www.cegid.com

3. Presentation of the SaaS Production Department

SaaS Production is a department of Cegid Group whose mission is the provision of applications in SaaS mode (Software as a Service) for Cegid customers.

The main tasks of this team are:

- To create the necessary architectures for hosting applications and data
- To operate the physical infrastructures, software and network
- To ensure applications are operating properly
- To ensure the technical support activities related to SaaS activities

4. Risk management

Cegid SaaS Production teams have implemented a risk management based on the principles of the ISO 27005 standard.

The first step is to conduct a risk analysis.

An action plan to deal with the risks is then constructed in connection with all the teams.

Regular monitoring and review of the action plan are organized during operational and strategic committees under the responsibility of the CISO and his team.

5. Information Security Policy

Cegid's SaaS activities are supervised by an Information Security Policy (ISSP). This policy was established in 2008 and is reviewed every 18 months. It is based on principles and best practices of the ISO 27001 and ISO 27002 standards.

The security policy is published in Cegid's in-house document management tool and every member of staff concerned is automatically notified of revisions.

This policy is confidential and not releasable. This document follows its plan and information that can be communicated.

6. Organisation of Information Security

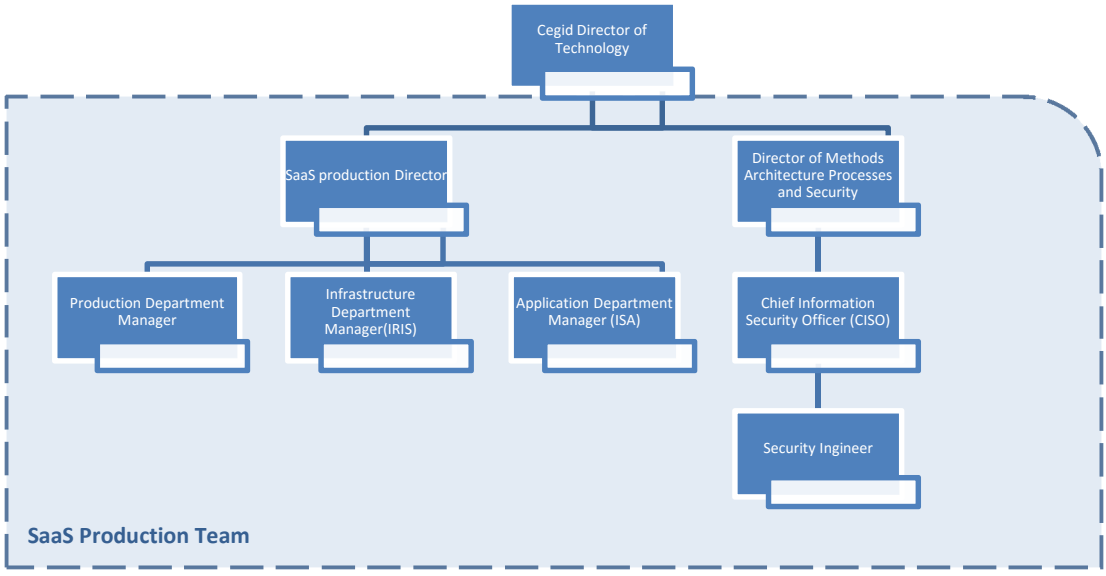
6.1. In-house Organisation

6.1.1. Roles and responsibilities

Security responsibilities have been defined and assigned.

A CISO is named for Cegid's SaaS activity: Mr Sylvain FOUREY

The actors involved in information security are:



6.1.2. Governance

The governance bodies are in place at strategic level (Strategic Committee of Information Security) and operational level (Operating Committee of Security Information).

These bodies meet regularly to follow up on topics related to computer security and reports are stored in the document management system.

6.1.3. Relationship with organisations and authorities

Cegid is a member of CLUSIR (Regional Clubs for Information Security) Rhône-Alpes, the OzSSI (Zonal observatories for the Security of Information Systems) and maintains relations with the authorities to monitor developments in the field of information security.

6.1.4. Security monitoring

Security monitoring is in place and conducted within Cegid's SaaS activity. It helps prevent risks specifically related to SaaS activities.

Cegid also relies on the services of a company specializing in security monitoring (CERT) to increase its research capacity. This multiple research method allows to cross-reference information and to have more suitable and relevant results in the specific context of SaaS.

6.1.5. Mobility

The SaaS Production management teams have the ability to connect remotely. Such access must be made using a secure connection (VPN or secure access interface). Strong authentication based on OTP token (One Time Password) is required to connect remotely.

7. Security related to human resources

7.1. Recruitment

Cegid's recruitment process includes a number of checks (criminal records, diplomas ...) from candidates in accordance with the regulations applicable in France.

7.2. Privacy Management

The entire SaaS Production personnel are sensitized to security.

Each contract includes a confidentiality clause. Below is an excerpt of employment contracts:

> Nous vous rappelons que l'accès à ces informations, en raison de l'importance stratégique et du caractère confidentiel qu'elles revêtent pour le Groupe CEGID, constitue une responsabilité qui n'est attribuée qu'à un nombre de collaborateurs très restreint.
> Dès lors, il vous appartient de vous assurer de la confidentialité des informations et de cet accès et d'interdire, de quelque manière que ce soit, directement ou indirectement, à quiconque qu'il soit salarié ou non de la Société CEGID, la transmission des informations ou l'accès à ces informations.

In addition, our rules of procedure, signed by each employee on recruitment, also stipulate the rules of confidentiality and the proper use of communication tools such as email.

Moreover, there is an awareness plan related to confidentiality and professional secrecy led by the CISO of the SaaS production department.

7.3. Competency Management

7.3.1. Awareness

New employees of the SaaS Production department follow an integration path that includes a security and confidentiality awareness plan provided by the CISO or a member of the security team.

Regular awareness plans, for the entire SaaS Production staff are then carried through during face-to-face sessions or information e-mails.

7.3.2. Competency Management and Training

In order to maintain the expertise, to identify training requirements and to facilitate knowledge sharing, Cegid has set up a competence management program for the entire SaaS Production staff.

8. Asset Management

8.1. Inventory

Assets of the SaaS perimeter are inventoried in the SaaS platform management tools. A set of characteristics and properties are stored such as the identifier, configuration...

An automated update process reconciles the inventory and assets present in the SaaS perimeter.

8.2. Asset identification

The identification of assets used in the provision of SaaS services is based on a naming convention formalized without distinctive sign, to establish a direct relationship with customers.

8.3. Managing removable media

The SaaS Production management teams do not normally need removable media to exploit Cegid's SaaS platform.

If removable media, such as a USB stick, is necessary to achieve customer data transfer, this data is encrypted (cf. § Cryptography).

8.4. Asset disposal

Asset Disposal is subject to a specific process for deleting confidential data. This process allows secure deletion or physical destruction of the media that have contained confidential data.

Concerning Cegid's Private Cloud, media (hard disks, tapes) containing data are physically destroyed (grinding or punching) when disposed of or because of a breakdown. A report is provided in follow-up security committees with the supplier.

Paper documents containing confidential information are shredded before being discarded.

9. Access Control

9.1. Password policy

Each user is authenticated by a unique ID and strong password.

Passwords management, for the managers of Cegid's SaaS production team, is subject to a strict security policy:

- Minimum size: 10 characters
- Complexity: letter, number and symbol
- Change frequency: every 60 days
- No reuse of the last 24 passwords
- Lock out after 5 attempts (unlock by an administrator of the SaaS Production team)

The password policy for the users of Cegid's SaaS clients is as follows:

- Minimum size: 8 characters
- Complexity: letter, number and symbol
- Change frequency: every 90 days
- No reuse of the last 24 passwords
- Lock out after 5 attempts (unlock by an administrator of the SaaS Production team or by the user via an online password management tool)

9.2. Rights management

Rights management for the SaaS Production teams are based on the "least privilege" principle. Each team has only the rights necessary to the activity it performs.

The requests for rights (addition, modification, deletion) are made through workflows with validations by the security team.

9.3. Access removal

Access removal is related to the HR processes of employees leaving the company. These actions are monitored and traced through the internal workflow tool.

9.4. Rights review

A review of rights for the administrators of the SaaS Production team is carried out yearly by the SaaS security team. This action allows to check and ensure the correct application of security regulations.

10. Cryptography

10.1. Data transfer

Data is encrypted during transmission with secure protocols. The SaaS platform uses the following protocols:

- HTTPS (TLS)
- SFTP (SSH)

If confidential data must transit on the links or insecure media (eg email, removable media), they are required to be encrypted in accordance with the rules in use (see § Encryption).

10.2. Certificates

In order to ensure the highest level of security, the HTTPS certificates used by Cegid come from public and known certificate authorities. The certificates currently implemented use 2048bits keys and a SHA256 signature in accordance with the best practices.

10.3. Encryption

The rules regarding the length of the encryption keys are:

- Asymmetric encryption: greater than or equal to 2048bits
- Symmetric encryption: greater than or equal to 128bits but 256bits is recommended if the system accepts it.

Cegid's SaaS Production team uses encryption software based on AES256 to create secure archives.

10.4. Mobile workstations

The mobile workstations of Cegid's SaaS production administration teams are equipped with a security suite for full disk encryption. It uses AES256 encryption protocol.

11. Physical and environmental security

11.1. Location

The datacenters used by Cegid are located in France. They are distributed in the Paris and Lyon regions and in Montpellier.

The control center of Cegid's SaaS activity is located in Lyon, at the headquarters of the group.

11.2. Datacenter security

To provide an optimal level of security, the datacenters used by Cegid are all certified Tier III+

The datacenters located in the Paris region and the one located in Montpellier are certified ISO27001.

The main features are:

- Electricity
  - Double general supply
  - Inverter
  - Double supply in the rooms
  - Emergency generators with fuel reserve
- Air conditioning
  - Double air conditioning system
  - Cooling optimized by false floors
- Fire Protection
  - Double detection circuit
  - Extinction by Gaz
- Security
  - Security perimeters around the buildings
  - Alarm with onsite surveillance
  - Guarding 24/ 24, 7 /7
  - CCTV
  - Secure internal areas with access control
  - Access on list and badge
  - Entrance one-person security-door or monitoring by a guard

11.3. Equipment security

A set of measures and principles have been taken in the design of the infrastructure to provide the optimum level of availability and integrity of Cegid's SaaS services.

The main rule is to avoid SPOF (Single Point Of Failure) in equipment or links.

For example:

- Redundancy at the level of physical servers
  - Power Supplies
  - Fans
  - Network Cards
  - Management Cards
  - SAN access optical fiber Cards
- Redundancy at the network level
  - Switches
  - Access Routers
  - Duplication of LAN links
  - redundancy inter-site links
  - multiple operators
  - High availability firewall
- At the storage level
  - Redundancy of SAN optical switches
  - Redundancy of SAN controllers
  - Duplication of paths to the SAN
  - Use of RAID principles to optimize and secure the data
  - Hard drives in "spare" to transparently address physical failures
- Virtualization
  - Use of a fully virtualized system infrastructure
  - Immediate move of virtual machines in case of an overactive hypervisor
  - Automatic move of virtual machines in case of a failing hypervisor

11.4. Access control

Access to secure physical facilities that host critical systems and network equipment is restricted to authorized personnel only. Each access is tracked and validated by a dedicated process. The room access logs are reviewed quarterly at the Security Control Committee.

11.5. Clean Desk

A clean desk policy is in place on the premises of SaaS teams. Documents, medias, removable files containing confidential information should be placed out of sight, in locked drawers when not in use.

12. Security related to operations

12.1. Data

12.1.1. **Data ownership**

There is no delegation of data ownership when using Cegid's SaaS services. The customer remains the owner of his data, as specified in the Subscription Services Agreement.

12.1.2. **File Security**

Data files are stored in folders dedicated to each of our clients. These directories are protected with NTFS security type.

This is to ensure security, partitioning and sealing between each customer.

12.1.3. **Database Security**

For its databases Cegid uses well-known standard systems such as Microsoft SQL, Oracle or MySQL.

The selection of major players in the database field enables Cegid to rely on confirmed publishers and on an active community to maintain the database management systems at its optimal level.

12.1.4. Date Encryption

Data is secured during their transfer between the user workstation and the Cegid SaaS platform, using HTTPS or SFTP encryption protocols.
The data is then stored in the SaaS production environment, a secured areas, both in terms of storage and backups. In this case, date encryption is not necessary.

12.1.5. **End of contract**

The terms of customer data conservation and deletion, following the termination of a contract, are detailed in the Subscription Services Agreement.

12.2. Antivirus

All the server infrastructure is protected by a centralized antivirus and antimalware solution. The hub server controls at least once per day the availability of updates pushed by the publisher. They are then broadcasted on all servers.

A monitoring of the antivirus is integrated into the supervision of the Cegid SaaS platform and is the subject of indicators reviewed at the committees related to information security.

12.3. Backup

12.3.1. Backup policy

Cegid's SaaS Production team focuses on the data of our customers. In order to ensure the integrity and availability of the data, Cegid has implemented a high-performance backup system.

This system uses a leading backup software provided and maintained by IBM, our partner.

The principle chosen by Cegid is that of the double backup:

- A first backup is made from the production systems on a first dedicated infrastructure.
- Duplication is then carried out on a second dedicated infrastructure.

Backup infrastructures are not in the same datacenter as that of production. This process ensures an optimal level of availability and integrity while ensuring requirements of our RPO (cf. §RPO).

The backup frequency is specific to each offer and detailed in the Terms of Service of the relevant service.

12.3.2. Outsourcing principle

Outsourcing data is aimed at protecting the physical integrity of data media.

The datacenter that contains backup data is located more than 20km from the main site.

The data transfer between the two datacenters is done by means of a dedicated and private optical fiber connection.

12.3.3. Controls and restoration

A control of backup tasks is performed by the monitoring software. In case of an incident during a backup, an alert is automatically issued and dealt with by Cegid's SaaS Production teams.

As part of its regular operation activity, Cegid Production performs data restorations daily. These activities confirm the correctness of backups and restoration processes.

12.3.4. Retention principle

As a specialized publisher, Cegid knows perfectly the business and needs of its customers. This feature has helped establish specific backup retention times to each service offered.

These retention principles are detailed in the Terms of Service for each service.

12.4. Trace management

12.4.1. Collection of traces

Traceability on Cegid's SaaS platform is ensured by a tool that concentrates and correlates logged events. These are kept for 1 year for technical and operation purposes.

This tool allows to standardize the retention time of the information collected and ensures its security.

The information collected is for example the user's name his time of connection, disconnection, the application used, the source IP address...

12.4.2. Use of traces

The traces are collected for different purposes:

- To reply to regulatory constraints linked to Cegid's business
- To follow the health status of Cegid's SaaS platform and to quickly identify any event that may cause a degradation of service.
- To produce anonymized statistical information on the provision of the service.

The use of the statistics and information generated by the traces is governed by the Subscription Services Agreement.

12.5. Supervision

12.5.1. Principles

All services and Cegid's SaaS platform are supervised by centralized tools. These tools use either the SNMP protocol or robots specifically developed to retrieve information from all control points.

The SaaS Production teams can thus continuously monitor the health status of SaaS services and are alerted in real time in case of malfunction.

The tools are coupled to a SMS sending system to warn on-call duty teams during non-business hours (NBH).

12.5.2. On-call duty

The on-call duty team is responsible for monitoring and intervening on the SaaS platform 24 /24 and 7 /7. It is composed of specialists representing all fields of competence in SaaS Production.

12.6. Update management

12.6.1. Management of installed software

Cegid uses software that enables to make an inventory and to master all software installed on the SaaS platform and on administration workstations.

12.6.2. System update

System updates are performed through a centralized console.

The principle adopted by Cegid to achieve both critical and security updates is the following: updates are deployed on a set of controlled environments during 7 consecutive days following the release of a patch. This allows to check if the patch does not cause any integrity and availability problem for the services delivered to customers. If no problems are detected, the installation is deployed throughout the platform during the following seven days.

12.6.3. Application update

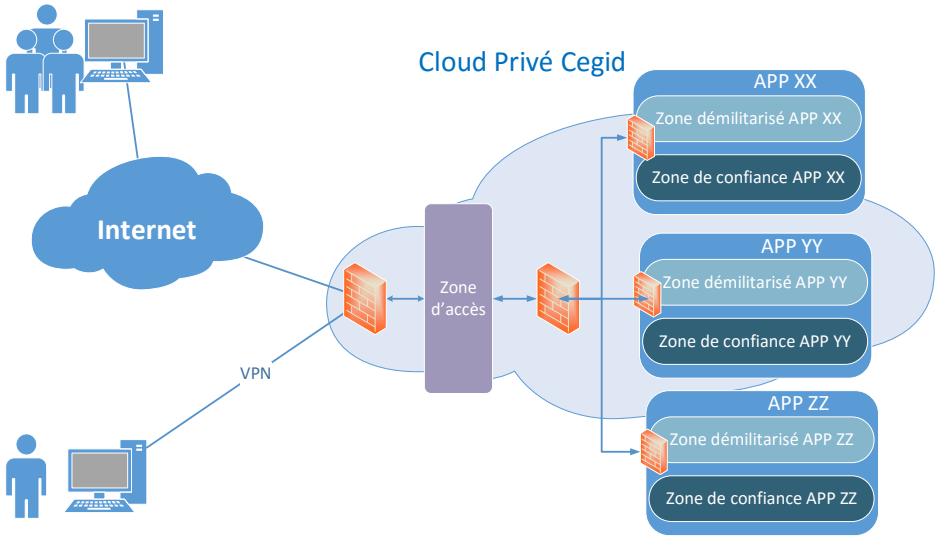
Cegid implements industrial, technical and organizational processes to manage application updates according to the service agreements defined in the Terms of Service for its SaaS solutions.

13. Communications Security

13.1. Technical architecture

The infrastructure of Cegid's SaaS services is organized in security and application zones. This principle provides efficient security adapted to current and future needs.

The flows between each zone are controlled by firewalls.



Caption

Bubble APP XX, YY, ZZ: Application bubbles corresponding to a set of grouped zones in order to run an application independently and securely. This architecture ensures the insulation between different SaaS services.

Trusted Restricted Zone (TRZ): Secure area that contains the applications and production data.

Demilitarized Zone (DMZ): Intermediate zone that contains the front service of the applications. This area enables to create a security area between the access areas (internet and VPN) and the trusted restricted zones.

13.2. Telecom Access

There are two access modes for Cegid's SaaS services:

- VPN
- Secure Internet

13.2.1. VPN

Cegid provides its customers with the possibility of using a direct, optimized and secure access to its SaaS services through a private network solution. The availability and characteristics of this network are specified in the technical requirements of each SaaS solution.

To prevent the risk of downtime, VPN access points are doubled and the material used is redundant.

13.2.2. Internet

Cegid has its own public IP addresses as well several internet access from different providers to overcome any failure of a supplier and thus provide its customers with the expected level of service.

All communications provided by Cegid are secure. The flows pass via HTTPS and SFTP.

13.3. Security equipments

13.3.1. Firewall

Firewalls are present between each security and each application zone (see §Technical Architecture).

Flows from the outside go through several layers of firewalls before reaching the requested service.

Direct flows towards the trusted zones are not allowed, they must go through the demilitarized zones (DMZ).

13.3.2. IPS

IPS sensors are present at the top of the network to scan all inflows and outflows to and from Cegid's SaaS platform. Their role is to detect and block any abnormal flow and malicious traffic.

The probes are provided by the security experts of the publisher with updates of attack signatures.

13.3.3. Vulnerability scanner

Scans on the entire Internet perimeter of the SaaS platform are run monthly using a vulnerability scanner managed by the security team of Cegid's SaaS Production. These scans are used to verify the proper configuration of hardware and software in order to prevent vulnerabilities.

The results are reviewed and are the subject of specific action plans.

13.3.4. Load balancer

The availability of the SaaS services is ensured by multiple load balancing systems. These systems are available to address a malfunction, a component failure or temporary unavailability while the systems are being updated.

14. Acquisition, development and maintenance of information systems

Securing the developments is a major challenge for Cegid.

Cegid has implemented, within each development team, a community of developers who are referents in the field of security. This allows to capitalize on the topics of security and to ensure the dissemination and implementation of best practices (type OWASP).

A development committee and working bodies, between the different "Cegid" staff involved in the life cycle of products, ensures continuous improvement.

A specific security watch is made and regular newsletters about updates and improvements are sent to the teams.

15. Relations with the providers

Security is taken into account when Cegid is signing a contract with providers. A document describes the security requirements, roles, responsibilities and indicators among stakeholders.

A follow up on security measures and a review of the indicators is conducted quarterly with the suppliers.

Audits are organized or certifications are required to certify that the information system of our providers is secure.

16. Management of incidents related to the security of information

16.1. Management of security incidents

The management of security events is equipped with a workflow in the management tool of Cegid's SaaS activities. The principle is based on the best practices described in the ISO 27001 and ISO 27002 standards.

It contains the following steps:

- Reporting
- Assessment
- Reaction to the incident (containment, communication to interested parties)
- Treatment of the incident (Corrective Action)
- post incident treatments (implementation of preventive actions)

Once the security incident impact is evaluated, the clients and / or partners will be promptly contacted to receive an update.

Depending on the nature of the action plan, Cegid will also contact the corresponding internal teams to organize the resolution of the incident.

16.2. Crisis management

A crisis management plan exists for Cegid's SaaS activity.

Crises scenarios are described in specific management processes and reaction to crises sheets. A crisis management directory is common to all scenarios.

A regular review is organized to reflect the changes and associated risks in Cegid's SaaS business.

17. Management of business continuity

17.1. Control continuity

A business continuity plan is set for the management and control of SaaS (infrastructure, applications ...) services by the SaaS Production teams.

17.2. BCP & Resilience of SaaS services

Cegid SaaS platform is designed to be resilient. The major risks are covered by the principles set out in the paragraphs "Security Organization", "Characteristics of datacenters," "Security of equipments", "Backup", "Technical Architecture", "Telecom Access" and "Security equipments".

17.3. RPO & RTO

17.3.1. RPO

RPO: Recovery Point Objective

Cegid guarantees, as standard, a RPO of 24h for all the data of its customers. When the DRaaS service is activated, a different RPO may govern the Service. In this case, the RPO is defined in the corresponding Terms of Service.

17.3.2. RTO

RTO: Recovery Time Objective

Cegid does not define an RTO in its Terms of Service, as a standard. In case of a serious incident resulting in a prolonged service interruption, Cegid is committed to restore the Service, as soon as possible, based on the most appropriate backup.

When the DRaaS service is activated, Cegid is committed to an RTO defined in the corresponding Terms of Service.

17.4. DRaaS

The DRaaS Service allows the customer to benefit from a recovery of activity of all or part of their SaaS service, on a backup site, in case of a major disaster (destruction) on the production site resulting in prolonged unavailability of more than 24 hours of service and which prevents Cegid from determining with certainty a deadline for the resumption of activity at the production site. The Cegid DRaaS Service is based on a technical solution for continuous replication of customer data to the backup site.

The execution conditions (RTO, RPO, scope, process etc ...) are described in the corresponding Terms of Service.

18. Compliance

18.1. Standards & regulations

18.1.1. ISO 27001

SaaS Production teams use the ISO 27001 and ISO 27002 standards to design and operate Cegid's SaaS platform.

In order to provide an architecture and infrastructure that meets the state of the art in terms of security, Cegid relies on data centers and related services that are certified ISO 27001.

18.1.2. ISO 9001

Cegid's cloud infrastructure providers are ISO 9001 certified.

18.1.3. CNIL (French Privacy Protection Authority)

18.1.3.1 Cegid acting as a Subcontractor

The Customer is informed that it is for him to make the necessary procedures, declarations, authorization requests under the laws and regulations concerning any treatment carried out and data processed from the Service and in particular those provided by the C.N.I.L. concerning the processing of personal data. It is recalled that according to the meaning of Law No. 78-17 of 6 January 1978 called Data Protection, Cegid acts as subcontractor, on the instructions of a Customer, who is described as responsible for processing the data implemented through the Service.

More generally, it is up to the Customer to comply with all local laws if a specific process of administrative declaration relating to personal data is required.

The data collected by Cegid, as part of its SaaS business, are declared to the CNIL according to the laws in force on French territory.

18.1.3.2 Cegid acting as a Data Processor

As part of its activity as a SaaS service operator, Cegid could will make the necessary procedures, declarations, authorization requests under the laws and regulations concerning any treatment carried out by Cegid when Cegid is considered as responsible for them by the National Commission and Freedom (C.N.I.L.) and the French legislation.

Are exclude from Cegid actions scope the procedures, declarations, authorization requests that are under Customer responsibility and where Cegid as considered as subcontractor.

18.2. Internal Audit

The Cegid SaaS operation is audited yearly by the internal audit department of Cegid group. The following activities are performed:

- Reviews security risks
- Recommendations for improvements with action plans
- Evaluation of security indicators for management

Cegid internal audit reports are confidential, thus they cannot be communicated to the Clients. In the event of a security breach, Cegid commits to contact the affected Clients as soon as possible.