cegid

Terms of Service

Cegid Wittyfit

11/30/2023

www.cegid.com

CONTENTS

HISTORY OF CHANGES AND VALIDATIONS

Nature of the changes	Version	Date
Document creation	01	03/20/2023
Format update	01.1	11/30/2023

Audited by

Date	Name, position
04/01/2023	Alexandre Blanc, Cegid HCM Solution Architect
04/01/2023	Flora Brousse, Cegid HCM Product Marketing Manager

Approved by

Date	Name, position
04/01/2023	Laura Martineau, Cegid Wittyfit Customer Success Director
04/01/2023	Thibault Perret, Cegid Wittyfit R&D Manager

Distribution list

Person or group
Cegid Wittyfit Customer
Cegid Wittyfit internal

1. INTRODUCTION

1.1. Purpose of the Document

This Service document, an integral part of the Agreement, describes the specific provisions applicable to the Cegid Wittyfit Services. These provisions shall take precedence over the general provisions of the Agreement in the event of any contradiction, and/or complement the general provisions of the Agreement.

The applicable provisions for the protection of Personal Data are those contained in the Protection of personal data policy of the Agreement.

With regard to security, the Nominal Service is the subject of a Security Assurance Plan (SAP).

The purpose of this document is to describe the steps taken to ensure the following:

- quality of support provided by Cegid;
- quality of the processes for monitoring and escalating requests during the post-project RUN phase (Build phase);
- support RACI;
- description of the technical architecture of the Cegid Wittyfit application, both for the shared Customer infrastructure and for the Customer-specific infrastructure.

This document is updated whenever the technical environment of the service changes.

1.2. Modifications to this Document

Any update to this document will result in a new version. Changes are recorded and dated in the version history placed at the beginning of the document.

Minor changes will not necessarily lead immediately to a new version of the document. These will be integrated in the next version.

Any update to the document must be included in the history and represents a commitment by the parties involved.

In the event of an update to the document, the version published on the official Cegid website is the valid version. The version attached to the customer contract is used to check that there is no regression as set out in the contract.

This document is reviewed at least once a year. This review can lead to the issuing of a new version.

2. SUPPORT DESCRIPTION

2.1. Support Location

Cegid Wittyfit's Customer Care support teams are all currently based in France. Support requests can be submitted in English or French.

Support tickets must be issued via the ticketing tool contained in the Wittyfit platform. Users clicking on the pictogram "**?**" will be redirected to the Jira help center, a ticketing tool available via the Internet for all Customers with a Wittyfit contract.

All users of the Wittyfit platform also have the option to send an email directly to the support at the following address: wittyfitsupport@cegid.com.

2.2. Support Contract

Cegid offers a standard support package called "Open" (included in the license) for Wittyfit.

This allows you to:

- create support requests via the Wittyfit platform;
- access the product documentation via Jira;
- participate in webinar workshops providing training on the Wittyfit tool;
- participate in the Wittyfit user club.

In addition, this OPEN package provides access to:

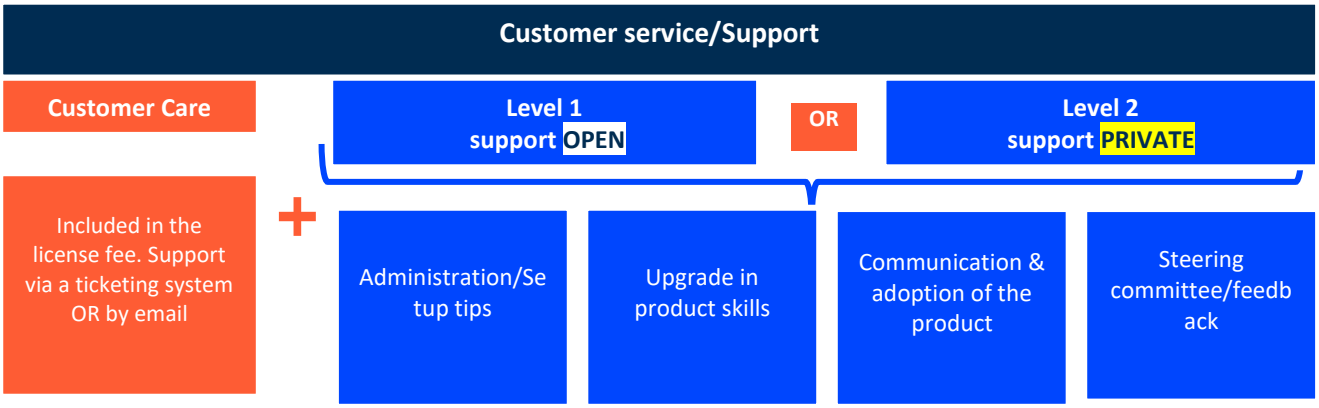
- a dedicated Cegid Wittyfit consultant;
- contextualized demonstrations of new features;
- steering committee/feedback;
- indicators for monitoring the service commitment.

Cegid also offers a second, optional level of support, the "Private" package. This package provides more sustained support.

You can request this service by contacting your sales representative.

This second level of support allows access to more detailed support, *see table below:*

Summary of our two support packages in the Run phase:



Details and differences between "Open" & "Private" support:

	OPEN	PRIVATE
Dedicated CSM contact (to guide you through the major steps: Kickoff, HR Call, organize training sessions and post-campaign feedback meeting)	X	X
Dedicated CSM contact for specific support: adapting questionnaires, creating questions, specific "manager" topics, etc.		X
Demo webinar* + Q&A		X 2 sessions*
Communication Plan support (Call with the customer's internal communication team => in order to discuss the different stages of communication: adapting the messages & the media)		X
HR Administrator training (adding and deleting employees, modifying assignments, adding manager rights, etc.)	X	X
Wittyfit* tool training (knowing the functionalities, how to interpret data, how to create action plans, how to integrate Wittyfit into managerial practice, etc.)	X 2 sessions / year **	X 5 sessions / year **

* 2 sessions for customers with more than 1000 employees. If fewer than 1000 employees, we only offer 1 session.

** **Training session packs:**

=> PRIVATE : **Pack of 5 sessions if above 1000 employees, otherwise 3 sessions.**

2.3. Access to Application Resources

Access to a customized resource bank is provided by your dedicated CSM contact. This is a space containing all the information you need to help you deploy Cegid Wittyfit within your organization: user guides, tutorial videos and other informative content.

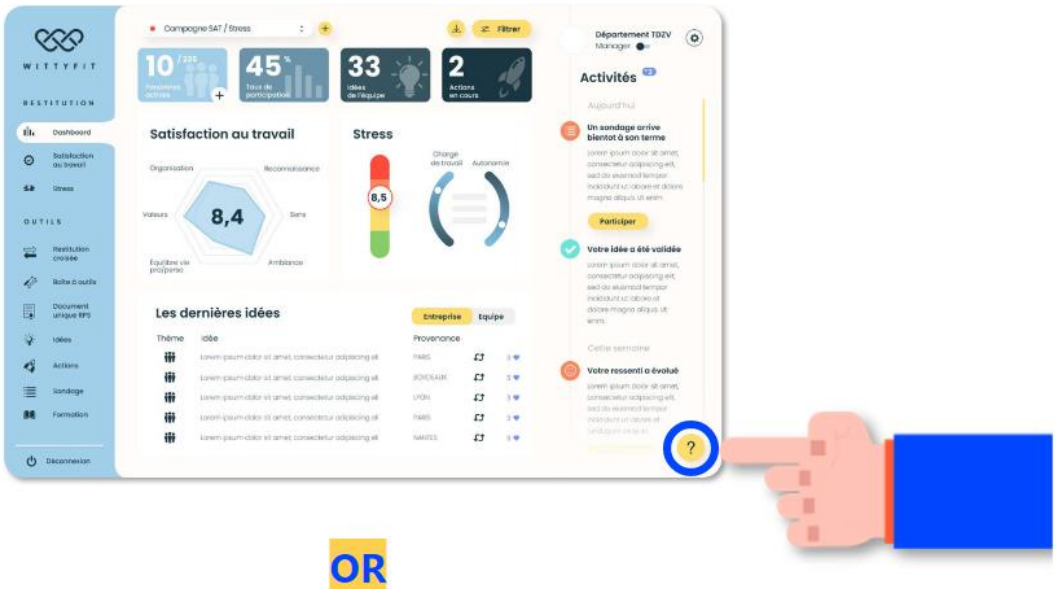
A second access can be provided to customers which they can share internally with other users.

2.4. Support Section

Support tickets must be issued via the ticketing tool contained in the Wittyfit platform. A support tool available for all users of the Wittyfit platform: employee access, manager access and supervisor access. The forms to create a new ticket are available:

- at the bottom of each page of the Cegid Wittyfit platform;
- on the Cegid Wittyfit platform login guides;
- by email: wittyfitsupport@cegid.com

Access Wittyfit support directly from the platform:



OR

By email: wittyfitsupport@cegid.com

Support for the Wittyfit solution is available 24/7; requests are handled by an operating team, Monday to Friday from 09:00 to 18:00 CET.

This tool is compatible with **Google Chrome** or **Firefox**. Browsers such as **Microsoft Edge** do not support all features of the Wittyfit platform pages and issues with slow loading or invalid pages may occur.

When submitting requests, users must specify the following information:

- the type and severity of the request,
- the title of the main request,
- the actions taken that led to the generation of the anomaly,
- a brief description of the problem,
- optional: a screenshot OR an attachment.

On closing the ticket, an on-the-spot evaluation is sent to the Customer in order to obtain their opinion and improve the quality of our service.

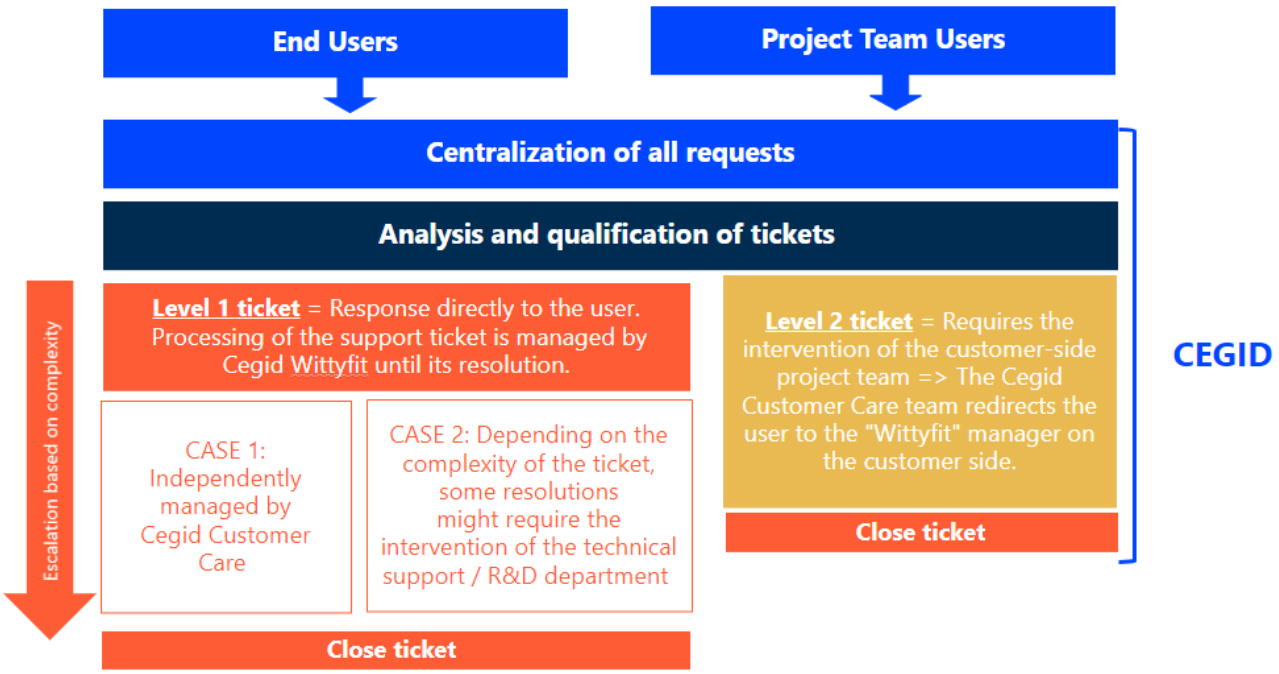
2.5. Support Ticket Worflow between the Customer and Cegid

2.5.1. List of Statuses

The following table explains the different JIRA (ticket management tool) statuses with the corresponding requester for the progress of the ticket.

Status	Definition	Responsible
New	The ticket is created by the Customer and sent to Cegid. This status is automatically updated by Zendesk when the ticket is created.	*Cegid*
Awaiting support response	The ticket is being processed by Cegid. This status is automatically updated by Jira once the party responsible is assigned or the Customer/user has added a comment.	Cegid
Awaiting customer/user response	The ticket is being processed by the Customer, This status is updated by Cegid when a response or additional information is required from the Customer/User. An email is sent by Cegid to the customer/users after ten (10) working days and two (2) reminders if there is no response from the Customer/User. The ticket will be closed automatically five (5) working days after sending the email.	Customer
Being processed	The ticket is being processed by Cegid. The ticket is being analyzed and/or processed by the technical support or R&D department.	Cegid
Awaiting validation	The ticket is being processed by the Customer.	Customer
Closed	The ticket is closed: • during validation by the Customer (automatic update); • on request for manual closure by the Customer to Cegid; Immediate closure	N/A

2.5.2. Workflow of Tickets between the Customer and Cegid Wittyfit



2.6. Contractual Definition of Bugs and SLA Policy

2.6.1. Definitions

An anomaly is a failure, incident, malfunction or abnormal behavior, which differs from the expected behavior as documented by the solution. The complete or partial unavailability of the application, or a degraded performance, which disrupts or interrupts the use of the solution, is also considered an anomaly.

The anomalies to be classified by Cegid are divided into three categories:

Critical anomaly:

- Malfunctions with no possible workaround.
- Interruptions in the testing of features and, more specifically, anomalies that:
    - Alter the data or its consistency.
    - Block the flow of business processes.
    - Produce results that cannot be used for business processes.

Major anomalies:

- Malfunctions that make it impossible to perform a task, but for which workarounds exist:
    - The system can be used, but with a reduced quality of operation.
    - The anomaly disrupts the execution of the action, but does not prevent Users from being able to test the other functions.

Minor anomalies:

- Malfunctions for which there are workarounds, and which do not affect other features:
    - The impact on the use of the application is insignificant.
    - Examples: anomalies that change the ergonomics of the system.

2.6.2. Cegid Standard SLA for Cegid Wittyfit

Anomaly resolution time

Service Level Agreements (SLAs) depend on the severity of the anomaly, as defined by the Customer:

	SLA in working hours	SLA in working days
Critical	Fifteen (15) hours	One and a half days
Major	Fifty (50) hours	Five (5) days
Minor	One hundred (100) hours	Ten (10) days

The working hours of the Cegid Wittyfit customer service team are Monday to Friday from 09:00 to 18:00 CET.

Service Level Agreements (SLAs) start as soon as incidents are submitted via a ticket to the helpdesk support platform during working hours, or at the start of the following day. The support period ends when Cegid confirms a final solution or workaround.

The time taken to process the "Awaiting customer response" ticket is deducted from the total processing time.

SLA period = (Acceptance date of the solution or workaround - Date created) - Time for which the ticket was "Awaiting customer response".

The SLA price is included in the license subscription price.

2.6.3. SaaS Availability

Cegid agrees to measure its service standards using the following indicator:

Definition:	Measures the overall service availability using the total cumulative downtime over six months (7 days a week - 24 hours a day)
Indicator objective:	99.5% availability (contractual agreement)

Calculation of availability (%)

[* Maximum availability over 6 months / (Maximum accessibility over 6 months - Time inaccessible (minutes))] x 100

* Total available minutes over 6 months = 60 minutes x 24 hours x 30 days x 6 months = 259,200 minutes

3. MAINTENANCE PROCESS IN THE RUN PHASE

3.1. Procedures

Support requests follow the procedure set out below. Depending on the type of request, steps 2 to 5 may be the final steps in the workflow.

Step	Act	Action
1	Customer	Create the request
2	Level 1 - Customer Care	File the request / Gather additional information
3	Level 1 - Customer Care	Qualification of complex subjects
4	Level 2 – R&D	Functional & technical analysis
5	Level 2 - R&D	Corrective action
6	Level 1 - Customer Care	Confirmation of the resolution

3.1.1. RACI Matrix for Support Activities:

- **R**: *Person Responsible*
- **A**: *Approver*
- **C**: *Consulted*
- **I**: *Informed*

Activities/Players	Customer administrator	Cegid Customer Care level 1	Level 2: Product/Technical support/Production	Customer Care Manager/Customer Success Manager
Declaration of requests	R, A	I, C		
Processing of the incident	C, I	R, A	C	C
Validation of the resolution	R, A	I		
Crisis management	C, I	R	C	R, A

3.1.2. Support Service Quality Control

There are several quality control measures to ensure the quality of the service:

- Continuous review of indicators by the Customer Care team, with improvement plans and follow-up actions;
- Daily review of ticket queues by the Customer Care team;

- Preventive alert rules in case of potential Customer escalation or breach of the SLA identified in the ticket management tool.
- Review of on-the-spot Customer evaluations and improvement plans;

3.2. Change Management Procedure

In every 2-week sprint, Cegid upgrades the Cegid Wittyfit version, with the distribution of patches and new features.

Each development is tested by the responsible engineer before being compiled into a version. A thorough qualification process is used for each version before rolling it out. Cegid uses a series of automated tests that must be successfully carried out before the new version can be presented to the rollout committee.

3.2.1. Version Management

New versions of the Cegid Wittyfit application are released in every 2-week sprint.

Cegid publishes documentation corresponding to the new features on the helpdesk.

By default, optional new features are deactivated on delivery. You can activate them by sending a request to the Cegid Wittyfit contact person, or by activating the new rights or configuration in the software.

Cegid's product teams may decide to distribute highly anticipated features or features that will significantly improve the use or operation of the software directly in production. In this case, the documentation is sent before going live, or a tutorial will be offered on the platform when logging in.

If for technical reasons a major feature with an impact on the ergonomics or the operation of the application must be distributed directly in production, the corresponding documentation is sent before going live. A reminder is sent two months before the feature goes live.

3.2.2. Maintenance Periods

1st Tuesday of the month:	18:30 - 19:30 CET patch management (weekly release, with a short production break to restart the application)
Twice a week:	Application maintenance window with service interruption of a few seconds.

Scheduled maintenance is announced at least one week before the maintenance date, via support or via our preferred communication channel with the customer.

3.3. Crisis Management Procedure

The objective of the crisis management process is to prevent and mitigate the damage of the crisis by triggering effective and regular monitoring of actions that cannot be handled by standard processes in order to quickly resolve the crisis.

Cegid's crisis management procedure includes the management of all types of incidents, including those with an impact on the service, but also security alerts. The procedure includes an escalation process that can escalate the incident to Cegid's executive management. The crisis management procedure is organized around a single interface created by the Customer Service team.

Crisis management processes are triggered under the following circumstances:

- in case of force majeure, of a blocking incident for which a workaround or a patch has not been provided within a reasonable period of time or of extended degraded situations over an unacceptable period of time: **CODE ORANGE**
- generalized critical incident or degraded situation: **CODE RED**
- all security alerts (known or potential) that endanger Customer data: **CODE BLACK**

3.3.1. Overview of the Crisis Management Process

The first action is to initiate the creation of a "crisis unit".

This unit identifies those Customers potentially impacted and establishes a communication plan to inform impacted Customers.

In the event of a confirmed code black, the Cegid crisis unit is activated and managed by the DPO and the ISSM. The unit identifies the Customers likely to be impacted and communicates with them through representatives designated in the project phase as security representatives (ISSM or equivalent).

In other situations (code red and code orange), the crisis unit includes, but is not limited to, the consultant(s) in charge of the incident, the incident manager, the Customer Service managers, the Cegid ISSM representative or a member of their team, a representative of the Cloud services and a representative of the R&D department. The crisis unit operates in the same way as for incident management. Regular communication, resolution and post-crisis feedback procedures are therefore in place.

The unit is dismantled once the problem is fully resolved, Customers are informed of the resolution and the incident report is created. The incident report includes a summary of the incident, the analysis with the original cause, the corrective actions and any preventive measures. Cegid's management then carries out an analysis and produces an improvement action plan (if necessary) based on the lessons learned from the incidents.

The crisis management process includes regular communication with the Cegid management and the executive management if required.

3.4. Contract Termination

3.4.1. Reversibility Plan

The agreement stipulates that data stored in the Customer's database belongs to the Customer (see the subscription agreement). In the event of termination of the contractual relationship, the Customer must therefore recover its accessible data through the features of the Service or ask Cegid to return its Data. Cegid will send the Customer all data and information received from the Customer as part of the execution of this agreement. To enable the Customer to use the data in question, it is sent in a standard market format chosen by Cegid.

3.4.2. Data Destruction Policy

In the event of termination of the agreement or a change of software platform, Cegid undertakes to delete all Customer data (including the database, URL and backups). Cegid shall provide Customers with a declaration of destruction of the data. The data is deleted 60 days after the end of the contract.

3.5. Request for Additional Services

A service request can be made by contacting your sales representative or your preferred Cegid Wittyfit contact.

A quote will be provided for additional services. The services offered are as follows:

- Additional training session(s)/Skills upgrades

- Translation of support materials into languages not offered by Cegid Wittyfit
- Translation of the Wittyfit platform into languages not offered by Cegid Wittyfit
- Installation and configuration of a question reading tool
- Ad hoc CSM/PS intervention by the day

4. HOSTING SITES

4.1. Hosting Locations

Cegid has chosen its hosting centers in order to allow its Customers to access the Cegid Wittyfit application and to comply with data privacy regulations.

Geographical area	Country	Main location (secondary locations)	Service provider
Europe	France	France Marseille MAR02 (France Marseille MAR03) (France Lyon LYO03 for backups)	Free Pro

4.2. Security and Confidentiality of Hosting Service Providers

We evaluate and select our hosting centers based on strict criteria of security, confidentiality, quality and availability. Having multiple centers allows us to be more responsive in setting up new Customer instances, manage load balancing, reduce risk and increase our capacity quickly and independently.

The Cloud provider and Cegid are bound by an agreement that includes a confidentiality clause. The list of persons authorized to access the data is reviewed regularly.

The legal structure of Cegid is based in France and the data centers of Cegid Wittyfit are located in France (Marseille). Cegid guarantees that the database is and will always be located in Europe for all European Customers. This guarantee also applies to backups.

Our hosting centers have the following in common:

- data centers designed with high levels of redundancy for very high availability solutions (tier III or equivalent);
- high-speed communication system based on a fully redundant long-distance fiber optic network;
- highest standards of active security;
- constant concern for energy efficiency and desire to limit any environmental impact.

The data centers used by Cegid have solid certification. For more information, please see the following documentation:

- Jaguar Network: https://www.jaguar-network.com/produit/datacenters/

5. TECHNICAL ARCHITECTURE

The Cegid Wittyfit application is based on a three (3)-level architecture:

- Users' workstations use a web browser and must have Internet access
- application servers respond to HTTPS requests
- data servers are only accessible from the application servers via an SSL connection. They host the database search engines, as well as the Customer data.

The underlying principles of Cegid Wittyfit's technical architecture allow:

- separation of Customers for security, confidentiality and availability purposes
- a high level of customization of each Customer's environment without impacting other Customers, while maintaining the uniformity of the software package
- hosting in data centers that meet Cegid's requirements.

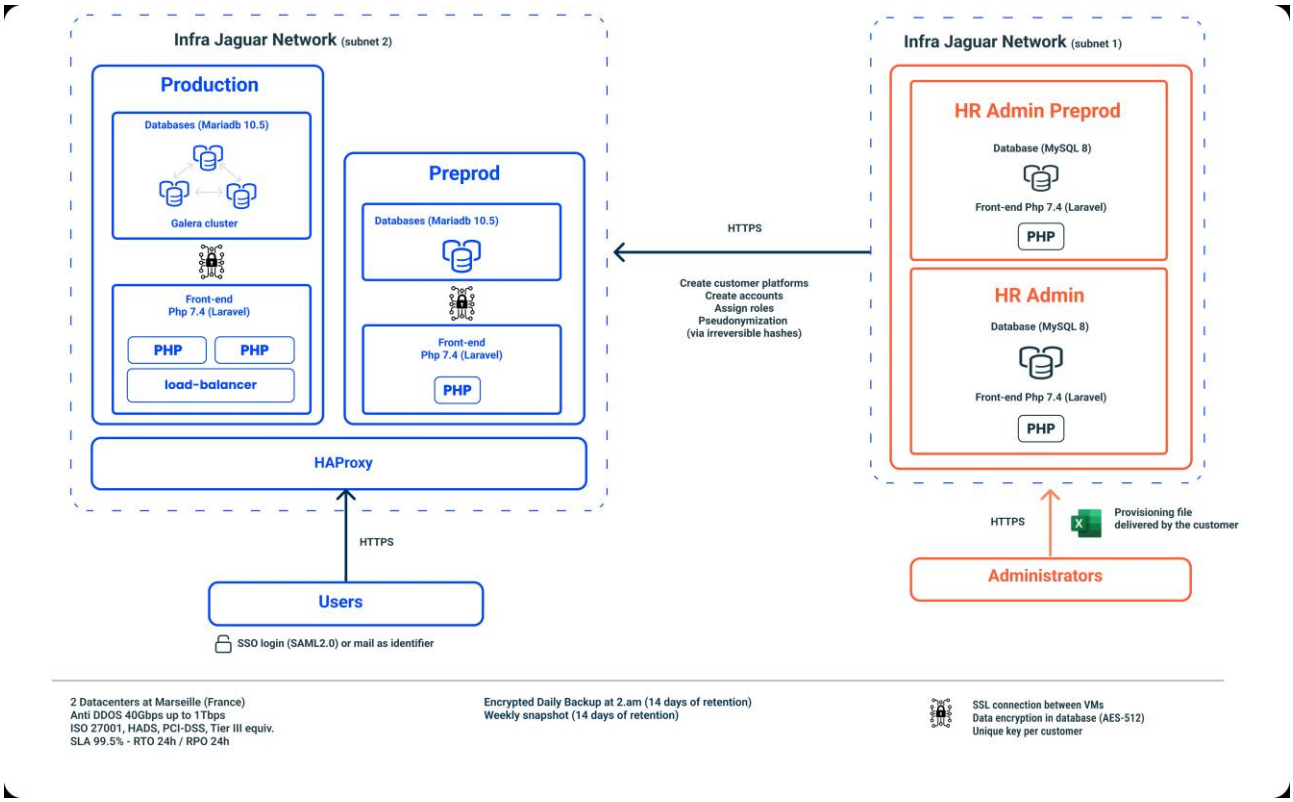
5.1. Application Architecture

The Cegid Wittyfit solution consists of 2 platforms separated into sub-networks to guarantee anonymity:

- **A user platform,** used by employees, managers and the HR department. This platform allows users to assess the different components of their job satisfaction. Managers and the HR department can navigate and analyze the results of different groups over time and by entity, geographical area (if defined) and sociological filter (if defined). We set a limit of anonymity below which returns are neither calculated nor returned. This limit can be configured upwards by the customer,but cannot be lower than 5. The platform allows data to be extracted in Excel, PowerPoint or PDF format.
- **An HR Admin platform,** mainly used by Cegid's integration teams, and which can be made available to the customers' HR teams. It can be used to load the user base, assign managerial rights and produce the analysis filter on the user platform. Data synchronization allows accounts to be pseudonymized on the user platform (hashing + salt) so that data sent by users cannot be directly linked to their identifiers.

5.2. Server and Network Architecture

Below is a diagram of the architecture used for hosting applications:



The application server virtualization technology is VMWare. The backup solution for its machines is Veeam.

All web servers are equipped with advanced HAProxy load balancing technology. All database servers are configured with synchronous replication with Galera Cluster.

The storage and archiving zone is physically separate from the production zone. The administration zone is only accessible to authorized Wittyfit administrators, after a series of 2 firewall filters and a strong authentication sequence. Each administrator uses a named and tracked account (Health data hosting (HDS) standard).

The data servers cannot be accessed from the Internet. Only the application servers have access to the data servers via encrypted connections within an isolated subnetwork cluster.

5.3. Technical Software Infrastructure

5.3.1. Infrastructure Components

The solution runs on a LAMP environment. It is structured as follows:

- at least 2 PHP 7.4 (Laravel) + Python 3.11 front-ends;
- isolated / customer databases (MariaDB 10.5, Redis) (possibility to instantiate a dedicated server);
- web application based on Angular 9+, accessible only in HTTPS.

The following is a summary of the major infrastructure components for the current product version:

For the PHP modules:

Component	Product	Version
Server operating system	Debian	10
Internet server	Apache	10.0
Application framework	PHP	7.4
Database engine	MariaDB	10.5

Concerned: HR administration, customer BO, user platform

For NodeJS modules:

Component	Product	Version
Server operating system	Debian	10
Internet server	NodeJS	12.22.x
Application framework	PM2	5.1.x
Non-relational database engine	Redis	6.0.16

For the Python modules:

Component	Product	Version
Server operating system	Debian	10
Internet server	Python	3.10.10
Non-relational database engine	N/A	N/A

5.3.2. Application Databases

The Cegid Wittyfit application is based on a group of databases:

Technical databases containing no User data

Database	Use	Instances
Main-Core	Database that lists all "tenants" of a physical site + technical logs	Centralized
HR-Core	Database that lists all the tenants for the HR admin + technical logs	Database accessible only to Cegid technical administrators

Databases containing User data

Database	Use	Instances
HR-Customer	Database of user lists and their assignment to groups, configuration of limitations to certain modules, and assignment of users to groups for sending email campaigns related to the platform's activity.	One database per Customer
Main-Customer	Database containing the customer's survey configuration, pseudonymized user data, data aggregations by groups, and technical logs related to the Customer's users. In this database, user identifiers are pseudonymized in the form of irreversible hashes.	One database per Customer

5.4. Multi-Customer Management

The Cegid Wittyfit application is available in the form of websites. Each Customer has its own sub-domain that can be served by a single or shared instance of the Web server. In this way, the product has a multi-tenant software architecture and all sub-domains point to the latest version of the application. Each tenant has a unique domain or a few unique domains that are matched against a unique tenant identifier.

Our architecture is multi-tenant, the multi-entity management in the database layer can vary but the application servers are pooled.

For the main databases (HR-Customer, Main-Customer) containing most of the individual information, the multi-tenant architecture allows each Customer to have their own database, co-hosted on shared SQL servers. In this case, the web server will connect to the tenant database to respond to a request.

The main reasons for this architectural choice are as follows:

- easier management of data security and confidentiality
- easier to back up and restore
- ability to customize the behavior of each Customer application instance, even if the same product is run for all Customers

5.5. Test Environment

A test URL can be made available to our customers at the beginning of the service to validate with our CSM team the compliance of the filter, and the correct consideration of the indicators and default questions.

The test environment is installed and managed as a separate environment from the production environment. It is managed as if it were the environment of a different Customer.

The test environments are used to test new functions before they are activated in production or to test an action. The data in the test environment is an anonymized copy of the production data at a given time, and is therefore older.

By default, all data in a test database is anonymous and empty of any content. If the Customer makes a support request, Cegid may update the test data with production data using an account anonymization method (without attachments and with an appropriate level of anonymization).

Customers may ask Cegid not to anonymize the data in a test environment. However, in this case Customers are responsible for the confidentiality of the data and a longer delivery time is to be expected.

Test environments are not as widely available as production zones. In addition, Cegid reserves the right to temporarily interrupt these environments to perform various tasks (for example installations during working hours).

5.6. Mobile App

The Cegid Wittyfit mobile app is available on two mobile platforms: Android and iOS. The app can be downloaded from their respective app libraries.

The mobile app can be accessed in the same way as the web version. Single sign-on is supported as long as the customer has an identity provider in place.

The Cegid Wittyfit mobile app only provides a presentation layer. This means that no data is stored on the mobile device, except for the login cookie.

6. Access Management

6.1. Application Access Security

6.1.1. User platform

The user platform is accessible via the Internet in HTTPS. The customer chooses the sub-domain through which its users will access it (for example **society**.witty.fit). The user or manager must log in to the platform to access the service.

6.1.2. HR Admin

Accessible from the Internet, with 2-factor authentication by email. Access to data is based on the principle of least privilege.

6.2. Authentication

By default, authentication on the Cegid Wittyfit platform is by entry of a login and a password. SSO connection (SAML2) is available.

6.2.1. Customer Responsibilities

Customers are responsible for their own password policy. However, we inform you that the following policies may lead to serious violations of privacy legislation (such as the GDPR):

- reuse/cloning of passwords
- use of an algorithm to produce passwords
- use of a password known by more than one person
- use of leaked passwords or "easy to find" passwords such as "Admin1234" or "QWERty12@"
- level of complexity lower than the recommendations of the French data protection authority (CNIL): https://www.dpocentre.com/password-management-why-password-shouldnt-be-your-password/

In such cases, only the Customer would be responsible for the possible incident and its consequences.

6.2.2. User Platform

Several authentication mechanisms are available for Users working with the company:

- via login and password;
- via the user's email
- by single sign-on (SAML2 SSO).

It is possible to use several authentication methods on the same platform.

The session is managed entirely on the server. Only a session cookie is stored on the User's workstation.

6.2.3. Password Management

Default rules for passwords (email or personnel number login):

The password must be at least 8 characters long, and contain:

- 1 upper case letter
- 1 lower case letter
- 1 number

- 1 special character

Passwords are stored in a hashed base (argon2 + salting). The login details are also hashed (SHA512 + salting) for storage

At the Customer's request, Cegid Wittyfit can apply the following password policy:

- Increased password length
- Activate password rotation
- Duration in weeks between 2 password changes

The password policy for HR Admin requires 12 characters, and password rotation every 3 months.

We strongly recommend the use of single sign-on (SSO) if storing passwords in a database is an issue.

Lost/Forgotten Passwords. Users who forget their password and do not use single sign-on (SSO) should proceed as follows:

- If the identifier used is an email address, go to the Cegid Wittyfit login page to enter your identifier. Click on 'Forgot your password'. An email with a 6-digit code is sent to the user's email address. The user must enter this 6-digit code to prove that they are the owner of the email address. The user must then enter a new password before logging back in to the application.
- If you are using a personnel number to log in, go to the Cegid Wittyfit login page to enter your identifier. Click on 'Forgot your password'. Select and answer the secret question you chose when you activated your account. The user must then enter a new password before logging back in to the application. If the user entered an email address (optional) during the activation phase, the previous protocol applies.

6.2.4. Single Sign-On

If the Customer has an identity provider in place, then Users can be authenticated via single sign-on (SSO) based on SAML 2.0 protocols. For more details, please see the public documentation of the SAML 2.0 protocols.

6.2.5. Session Duration

The duration of a session depends on its specific use in the different Cegid Wittyfit modules:

- A session on the user platform lasts thirty-one (31) days.
- A session on Admin HR is terminated after sixty (60) minutes of inactivity.

6.3. Cookie Policy

When browsing our applications, cookies are stored on the User's browser. The purpose of cookies is to collect browsing information, maintain the user's session and allow them to access their accounts.

For a list of Cegid Wittyfit cookies, please see https://www.cegid.com/en/privacy-policy/.

With regard to data concerning cookies, Cegid is committed to complying with local regulations in each country, protecting the confidentiality of the data and complying with territorial obligations in terms of the location of data storage.

6.4. Roles, Rights and Accreditations

Cegid Wittyfit has an interface dedicated to the administration of roles, rights and accreditations.

6.4.1. Roles and Rights

Roles are used to define standard profiles with certain levels of access to Cegid Wittyfit features. Roles are fixed and defined, then assigned to Cegid Wittyfit Users. The rights assigned to roles are however a list defined in the product. Roles can be restricted on some modules depending on customer requirements.

6.4.2. Accreditations

User accreditation lists allow you to define who has the right to access the information of a given group. An accreditation list is a list of employees (called "managers"). Managers then have access to the combined results of the group(s) they manage (provided there are at least 5 respondents in the group). Accreditations can be completely reconfigured during the HR import in the Cegid Wittyfit HR admin.

User accreditation lists can be generated automatically from management rules (using an organization, for example). These lists are "updated" automatically. This means that if the content of the organizations changes, the lists will be updated automatically, usually within a few hours.

7. INTERFACES

In Cegid Wittyfit, data can be exported in CSV, XLSX, PPT or PDF format. The user base is imported by importing a CSV or Excel file. This chapter describes the underlying principles behind file exchanges, as well as the security aspects involved in these exchanges. Interface specifications are provided at the beginning of the deployment project.

7.1. File Import/Export

7.1.1. Operating Principles

The Cegid Wittyfit solution allows the user base to be imported from any system able to provide a CSV or XLSX file.

To keep the data synchronization efficient, we limit the service to a twice monthly synchronization. Imports can be "differential" or "full". An integrator will retrieve the file and import it to the HR admin platform. They verify the correct formatting and overall consistency of the data.

Access to each import is controlled by an access right and tracked in the administration interface.

The Cegid support team provides its customers with complete documentation on how to produce the file at the start of the project.

7.1.2. File Transfer Vectors

Customers can choose how the file will be sent.

Case of a customer who is not a Cegid HR solution user:

The Cegid Wittyfit team provides a secure drop box (openTrust-MFT, AES-256 encryption) allowing the customer to send the file to support. The downloaded file is stored in an encrypted container (VeraCrypt AES-256) on a drive encrypted with Bitlocker. The file is deleted following the update.

The Customer can make the file available on an SFTP platform and provide access to the technical team to set up an automated secure server-to-server recovery. The operator does not have direct access to the file, but sees the result of the import from the HR admin interface.

7.1.3. List of Available Import Formats

The file can be provided in CSV or XLSX format. Cegid Wittyfit provides complete documentation on how to produce the file at the start of the project. The format must not be changed during the project, otherwise it will require reconfiguration by our integrator.

7.2. Email Interface

The Cegid Wittyfit application sends emails using the classic SMTP protocol. Emails can be sent in HTML format or in plain text format if Customers cannot process HTML emails. Automatic emails are sent for 2-factor confirmation upon account activation or when changing password. The content of the emails can be configured when launching a campaign or scheduling an action evaluation.

The 2-factor validation emails come from the address wittyfitsupport@cegid.com

Campaign emails, action evaluations and activity summaries for managers come from the address noreply@wittyfit.com (with no linked account).

8. OPERATIONS

8.1. Operating Procedures

This chapter describes the most commonly used operating procedures during the service.

8.1.1. Purge

Purge of system logs. System logs are retained for ninety (90) days.

Purge of the application log. The application log contains the tracking data of the User's actions. This log stores one (1) year of data, older data is purged.

Purge of files downloaded from secure SFTP. The files stored on the server after SFTP exchange are stored for a maximum of thirty-one (31) days.

8.1.2. Scheduled Tasks (Batch Tasks)

A certain number of batch tasks are scheduled in the standard application (sending emails, calculating notifications, purges, updating of coefficients).

Each task can be run using a standard scheduler that can run an online command task. Cegid is responsible for managing the schedulers.

8.2. Data Management

8.2.1. Data Backup

This chapter applies to production databases. The databases of the test environment are not backed up.

Organization of Backups

Database backups are performed based on a strategy requiring the best security and data integrity, as well as restoration time. These are online backups without any interruption of the database service.

The standard procedure provides for backups to be saved over rolling periods according to their type:

Action	Backup frequency	Conservation of backups
Complete daily backup of the databases	Once a day	Fourteen (14) days
Snapshot of application VMs	Once a week	Fourteen (14) days

The backup media operated by the subcontractor:

Action	Backup storage	Data replication
Private (Jaguar Network)	VM	Data is replicated within the same primary site and exported asynchronously to a secondary data center.
Private (Jaguar Network)	Storage disks	Data is replicated synchronously to a remote data center.

Only a very limited number of people have access to the database backups. These people, like all Cegid staff, are bound by a confidentiality clause. Our cloud provider also has a limited number of people authorized to access the backups.

8.2.2. Data Encryption

Data from free fields (ideas, actions, surveys) is AES-256 encrypted.

Data in Transit

Cegid encrypts all data transfers via HTTPS and TLS 1.2, and through the provision of certificates

Data at Rest

Logins and passwords are secured non-reversibly in the database through hashing and salting:

- in SHA512 + salt for the management of identifiers;
- in Argon2b + salt for the storage of passwords;

As a free option, Cegid provides a solution for encrypting text data in the database engine (AES-256). However, it should be noted that a 5% reduction in performance was observed.

8.3. Administration and Supervision

The platform is monitored 24 hours a day, 7 days a week. Performance monitoring and application supervision have been implemented and trigger alerts when issues are detected.

A processing and escalation process has been defined and is followed by the operational teams with the subcontractor. Supervision involves:

Operating procedures including the following tasks (not an exhaustive list):

- administration;
- operating system maintenance (disk space, logs, etc.);
- database maintenance;
- testing, qualification and rollout of security updates;
- application maintenance (logs and performance analysis);
- application availability monitoring;
- response time monitoring;
- monitoring of batch tasks for applications and systems;

Hosting providers are responsible for the tasks associated with the following:

- physical equipment (server hardware, network equipment, etc.);
- hypervisors;
- network;
- network bandwidth monitoring;
- hardware monitoring;
- monitoring of the platform load (memory, processors, disks);
- software updates for operating systems, databases and antivirus software;
- verification and qualification of backups;
- monitoring and updating of antivirus systems;
- maintenance of network equipment.

8.4. Business Continuity Plan

- Customer data is permanently replicated in two data centers 5km apart in Marseille. Daily backups are kept for 14 days in a data center located in Lyon (69).
- The recovery process is based on data replication, server redundancy and automated service restoration in data centers managed by our subcontractor Jaguar Network (Free Pro group).

9. REGULATIONS AND STANDARDS

9.1. General Data Protection Regulation (GDPR)

Below you will find a description of the applicable measures under the GDPR to assist Customers in their GDPR compliance with Cegid Wittyfit. Important: all data security elements are described in the Security Assurance Plan or in other chapters of this document; as a result, they are not mentioned here. However, they all relate to the GDPR in the sense that data security is a key requirement for all "data processors".

For the implementation of the GDPR requirements in its solution, Cegid Wittyfit, as a data processor, distinguishes two different profiles: employees and managers. Some of the requirements of the GDPR are not dependent on profiles, and some of them result in different product behavior depending on whether addressed to an applicant or an employee.

9.1.1. GDPR Requirements Applicable to all Personas

Respect for privacy from the design stage
The current agile development/software process covers staff training, formal code reviews, and tools that detect the need to apply best practices.

The principles relating to the processing of personal data as defined in Article 5 of the GDPR are taken into account by the design in the product development.

Privacy by default
By default, the data protection level is always set to the most restrictive level. For reasons of minimization, managers will never have read access to data for a group of less than 5 people (limit can be increased by the customer)

Data protection officer
Cegid has appointed a DPO given the nature of its activities.

Recording of processing activities
Cegid maintains a record of processing activities as a data processor

DPAs with subsequent data processors
Cegid delegates part of its activity to data processors. DPAs are signed between these processors and Cegid that contain clauses compliant with the GDPR. All procedures related to the ISO 27001 standard are in place. These procedures form part of our information security management system.

Sensitive data
Cegid Wittyfit does not collect sensitive data, such as that mentioned in Article 9 of the GDPR. As Cegid Wittyfit offers flexibility on the complements available for the data model, Cegid does not recommend that its customers define additional fields corresponding to "sensitive data", as defined in Article 9 of the GDPR. The use of the free field spaces is subject to reading and accepting a charter of good conduct, which provides a reminder of the precautions to take so as not to remove anonymity, not to transmit confidential or sensitive information (personal data, business, political opinion, etc.), and to ensure respect for everyone in any correspondence.

Notification of data breaches
Cegid has set up a data breach notification procedure. This procedure is defined, maintained and monitored within the framework of the ISO 27001 information security management system and the GDPR.

In the event of a breach of personal data, Cegid undertakes to notify the customer (the data controller) as soon as possible as required by the GDPR, so that the customer can then report the personal data breach to the relevant supervisory authority and the data subject within 72 hours, if such notification is mandatory. It is up to the customer to judge whether such a notification to the supervisory authority and/or the data subject is necessary.

Automated decision process
The Cegid Wittyfit application does not include any automated individual decision making or automated profiling function. All decisions are made by human users, who can use dashboards, KPIs, recommendations and analytics to make an informed decision.

Data anonymization
Cegid Wittyfit offers a "complete database" anonymization function. It is used when a production database is to be used for testing, debugging or training.

Information to be provided when personal data is collected from the data subject
It is the customer's responsibility to provide this information directly to their candidates and employees. Our solution offers our customer the possibility to provide this information, via a configuration.

9.1.2. Response to the GDPR Requirements on Employees

Right of access, right of rectification
The product provides the necessary features to access and modify employee data. Access to these features is managed by roles and rights, which can be assigned directly by the customer administrators.

Right to deletion
For various reasons, companies collect and process the personal data of their employees. Users can make a request to their DPO, or use the delete function from their profile.

There are prerequisites for data deletion:

- The end date of the former employee's contract must be in the past.
- The employee's record must be deactivated.

Legal basis
The data controller is required to determine the most appropriate legal basis for the Cegid Wittyfit solution prior to its implementation (art. 6.1 of the GDPR).

In the same CNIL reference document cited above ("*Référentiel relatif aux traitements de données personnelles mis en œuvre aux fins de gestion du personnel*" (Reference document on the processing of personal data used for personnel management) of November 21, 2019), the CNIL indicates with regard to consent that: "*Employees are seldom in a position to freely give, refuse or revoke their consent, given the power imbalance in the employer/employee relationship. They can only give their free consent if the acceptance or rejection of a proposal has no consequences for their situation*".

The CNIL therefore proposes other legal bases depending on the activity for the employees. This document contains a table to help the data controller to determine these legal bases.

9.1.3. Mapping of the Processing of Personal Data