cegid

Run Service

Statement of Work

01/09/2022

www.cegid.com/

CONTENTS

HISTORY OF MODIFICATIONS AND VALIDATIONS

Creation of the document	01	04/07/2018
Modification of SLA, addition of Zendesk status, update of Premium section	1.1	28/04/2020
Add escalation management, Advanced services	2.0	07/05/2020
Add new branding	3.0	11/01/2021
Update Support section, including new Helpcenter, change Approver	4.0	06/04/2021
Cegid Template	5.0	05/10/2021
Modify title, merge technical architecture specifics from former Talentsoft Technical Files, add approvers and auditors, rename document	6.0	04/02/2022
Add chapter Regulation & Guidelines	7.0	10/08/2022

Auditor(s)

28/04/2020	Anne-Claire Porter-Guillaumet, Customer Care Director
04/02/2022	Alexandre Blanc & Pauline Hubert, Solution Architects

Approver(s)

24/02/2020	Anne-Claire Porter-Guillaumet, Customer Care Director Cegid Talentsoft
04/02/2022	Francois Noel, Head of SaaS Cegid Talentsoft
04/02/2022	Pierre-Antoine Schaeffer, Head of Product

Distribution List

Person or Group
Cegid Talentsoft Customer
Cegid Talentsoft Internal

DOCUMENT PURPOSE

The Service Document is an integral part of the contract and explains the special provisions applicable to Cegid Talentsoft Services.

This document aims to describe the measures taken to ensure:

- The quality of the support provided by Cegid
- The quality of request follow-up and escalation processes during the post-project 'RUN' phase ('Build' phase).
- Support RACI
- Describe the technical architecture of the Cegid Talentsoft application, both for the shared client infrastructure and the client-specific infrastructure.

This document is updated whenever the Cegid Talentsoft service's technical environment changes.

SUPPORT DESCRIPTION

Support Location

Cegid Talentsoft Customer Care Support teams are based in France (Boulogne-Billancourt and Nantes), Netherlands (The Hague), Germany (Cologne), Denmark (Copenhagen), Sweden (Stockholm) and Canada (Montreal). Support requests can be made in French, English, German, Dutch, Spanish, Swedish and Danish.

Support tickets must be issued via the Help Centre on the Talentsoft Community (TS Community), a support tool available to all customers with a support contract via internet.

Support Contract

Cegid offers two types of support packages for Cegid Talentsoft:

Standard support package (included in the licence):

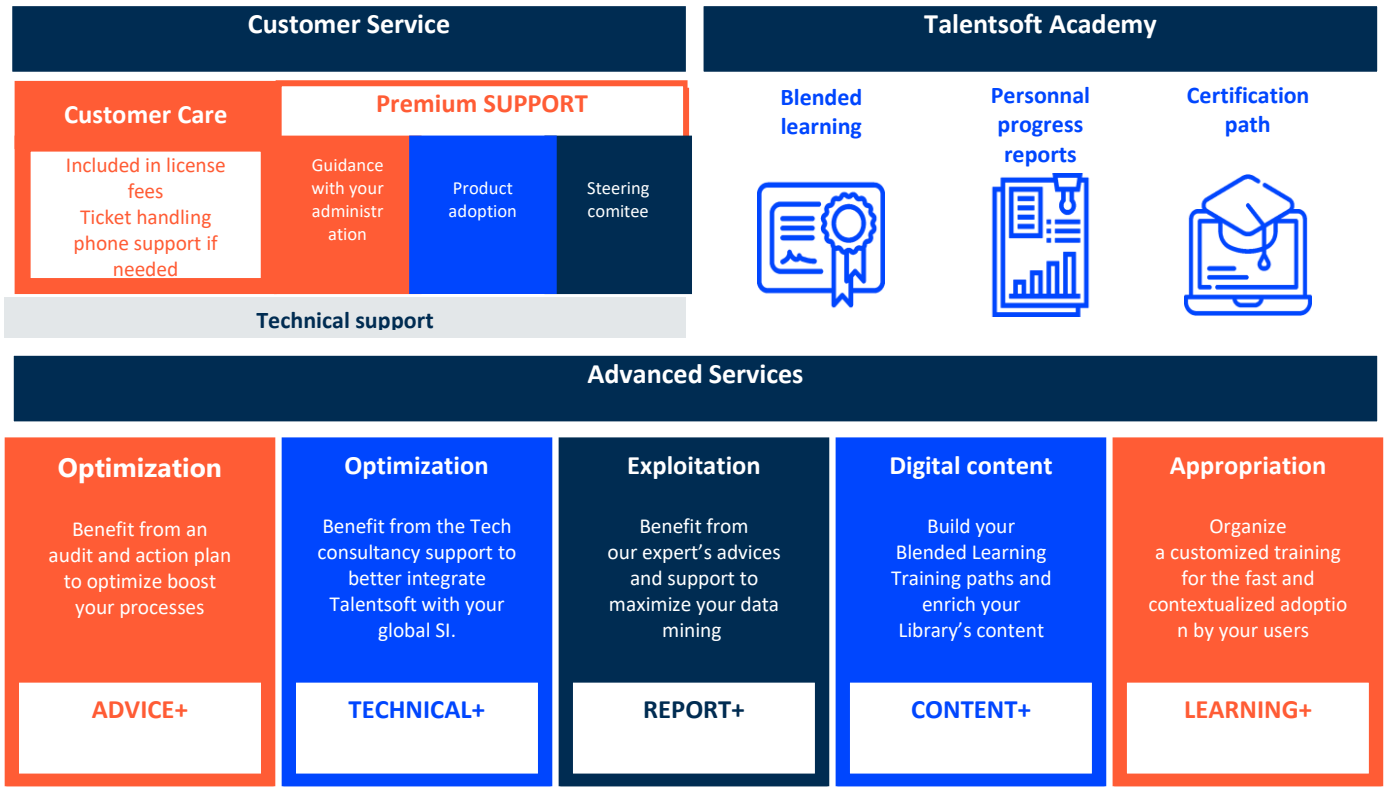
- Create support requests via TS Community
- Access new product features via TS Community
- Access product documentation via TS Community
- Participate in best practice workshops led by the customer community

Premium package (available as an option):

- Dedicated Cegid Talentsoft consultant
- Contextualised demos of new features
- Quality monitoring committee
- Steering committee
- Service commitment tracking indicators

In addition to these two types of support, customers in Run phase have access to Product Training via the Talentsoft Academy, and a wide range of service offerings which can be ordered after the project phase known as « Advanced Services ».

Summary of our Service offerings in Run phase:



Access to the Application Resources

The Talentsoft Community is a collaborative space where you can connect and collaborate with over 6,000 HR experts. It's also a go-to resource for product articles, FAQs, guides, tutorials, and other informative content as well as our latest HR news, feature, forums and events. It is also the point of entry in declaring support tickets via the Help Centre.

The documentation is classed by Cegid Talentsoft module.

The search functionality carries out searches through all available resources.

Customers can provide access rights to the Cegid Talentsoft document database for one or more users.

The Community user guide is accessible online on the TS Community.

Support Section

Support tickets are issued through the Help Centre section of the Talentsoft Community, a support tool available to all customers administrators. It is of the customer's responsibility to submit his requests. To create a new ticket, the forms are accessible:

- At the bottom of each article
- At the bottom of the Help Centre Page
- On "My Activities" page

TS Community is accessible 24/7; requests are processed by a functional team, Monday to Friday from 8:30 to 18:30 CET/ 9:00 to 17:00 EST.

This tool is compatible with either **Google Chrome** or **Microsoft Edge**. Browsers such as Firefox do not support all Community pages features and slow loading page or invalid page issues may be encountered.

When submitting requests, administrators must specify the following information:

- type and severity of the request,
- the action path taken to generate the anomaly,
- brief description of the problem
- full screen shot with date and time of the incident.
- Anomalies are described in section 3.5.

Configuration requests involve technical or functional actions that the administrator does not have the necessary access to carry out.

Upon ticket closure, a satisfaction survey is sent to the customer in order to obtain his feedback and improve our service quality.

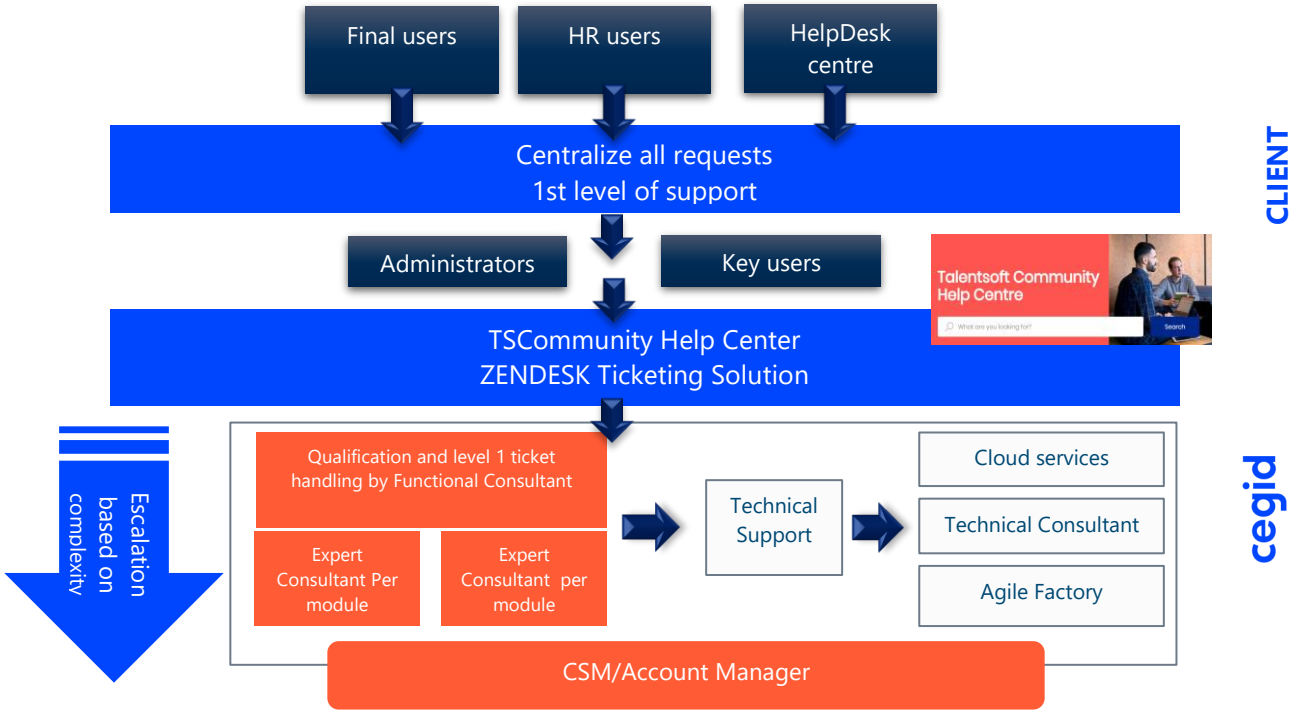
Ticket Workflow between Customer and Cegid

List of Zendesk Status

The table below explains the different Zendesk (ticketing tool) statuses with the corresponding owner for the progression of the ticket.

Status	Definition	Owner
New	The ticket is created by the customer and sent to Cegid. This status is automatically updated by Zendesk upon creation of the ticket.	*Cegid*
Open	The ticket is being progressed by Cegid. This status is automatically updated by Zendesk as soon as there is an owner assigned or the customer has added a comment.	*Cegid*
Pending	The ticket is being progressed by the customer. This status is updated by Cegid when a response or complementary information is required from the customer. The ticket will automatically be closed after 28 days and 2 reminders if no response from the customer.	*Customer*
On Hold	The ticket is being progressed by Cegid. The tickets is being analysed and/or processed by the technical support or R&D.	*Cegid*
Awaiting Delivery	The ticket is awaiting the deployment of a patch/ bug fix.	*Cegid*
Awaiting Approval	The ticket is being progressed by the customer . This status is updated by Cegid when validation is required by the customer. The ticket will automatically be closed after 28 days and 2 reminders if no response from the customer.	*Customer*
Validated	The ticket is solved. This status is automatically updated when the proposed solution is validated by the customer.	*Customer*
Closed	The ticket is closed: when validated by the customer (automatic update) upon manual closure request by the customer to Cegid automatically after a certain period if there is no activity on the ticket, regardless of its status: ***Awaiting Approval: Closed after 28 days (2 reminders)*** ***Pending: Closed after 28 days (2 reminders)***	*N/A*

Customer to Cegid Talentsoft Ticket Workflow



Contractual Definition of Anomalies & SLA Policy

Definitions

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

There are three types of severity:

Blocking anomaly:

- Malfunctions making it impossible to perform essential tasks, leading to a cessation in HR business activity
- Malfunctions that do not have any means of circumvention
- Interruptions in feature testing, and, specifically, anomalies that:

Alter data or their consistency

Block the flow of business processes

Produce unexploitable results for business processes

Major anomalies:

- Malfunctions making it impossible to perform a task, but for which workaround solutions exist:

System can be used albeit with decreased operating quality

The anomaly disrupts carrying out the action but does not stop users from being able to test the other functions.

Minor anomalies:

- Malfunctions with available workaround solutions, and that do not impact other features:

Impact on the use of the application is insignificant

Examples: anomalies that alter the system's ergonomics.

Cegid Standard SLA for Cegid Talentsoft

Anomaly resolution times

SLAs depend on the severity of the anomaly, as defined by the customer:

	SLA in working hours	SLA in working days
Blocking	15 hours	1,5 days
Major	50 hours	5 days
Minor	100 hours	10 days

Working hours for Cegid Talentsoft's Customer Service team are Monday to Friday from 08:30 am to 6:30 pm CET and 9.00am to 5:00pm EST.

SLAs begin the moment incidents are submitted via TS Community during opening hours or next start of business. The support period ends once Cegid confirms a definitive solution or workaround.

The time taken to process the ticket from 'Pending' and 'Awaiting Approval' is deducted from the total processing time.

SLA period = (Date solution or workaround accepted - Creation date) – Amount of time during which the ticket was 'Pending'.

The SLA price is included in the license subscription price.

Overall Availability

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

Definition:	Measures overall service availability using the cumulative total downtime over six months (7/7 – 24h/24)
Indicator objective:	99.5% availability (contractual agreement)

Availability calculation (%)

[* Max. availability over 6 months/(max. accessibility over 6 months - Inaccessibility time (mins))] x 100

*Total number of minutes of availability over 6 months = 60 mins x 24 hours x 30 days x 6 months = 259,200 mins

MAINTENANCE PROCESS IN RUN PHASE

Procedures for managing Incidents

Support requests follow the procedure mentioned below. Depending on the type of request, steps 2 to 5 may be the workflow's final steps.

Step	Act	Action
1	Customer	Create the request
2	Level 1 - Customer Care	Classify request / Gather complementary information
3	Level 1 - Customer Care	Qualification of complex subjects
4	Level 2 - Technical Support	Technical Analysis
5	Level 3 – R&D	Corrective Action
6	Level 1 - Customer Care	Resolution confirmation

RACI matrix for Support Activities:

- **R**: *Responsible*
- **A**: *Accountable or Approver*
- **C**: *Consulted*
- **I**: *Informed*

Activities/ Actors	Client Administrator	Customer Care Cegid Level 1	Customer Care Cegid Level 2	Level 3: Product/ Technical Support/ Production	Customer Care Manager/ Customer Success Manager
Declaration of requests	R, A	I, C			
Process incident	C, I	R, A	C	C	C
Validation of the Resolution	R,A	I			
Crisis Management	C, I	R	C	C	R, A

Service Quality Control

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

- Weekly KPI review by Customer Care management with improvement plans and action follow up,
- Customer satisfaction survey reviews and improvement plans,
- Daily review by control tower of ticket queues,

- Preventive alerting rules when potential customer escalation or SLA breach identified in the ticketing tool.

Change Management Procedure

Each week, Cegid performs a version upgrade for Cegid Talentsoft which involves delivering of patches and new features.

Each development is tested by the engineer in charge before being compiled in a version. A rigorous qualification process is used for each version before deployment. Cegid uses more than 25,000 automatic tests that must be successfully passed before the new version can be presented to the deployment committee. The Customer Service Management has final approval rights for deployment to production.

Versions go online each Monday evening after 6pm CET, without fail. Test and Production environments are both deployed at the same time.

Versioning

New versions of the Cegid Talentsoft application are released on a weekly basis.

Cegid publishes the documentation corresponding to the new feature(s) on the TS Community.

By default, new features are delivered in deactivated mode. They can be activated by issuing a request to Cegid Customer Care or by activating the new rights or configuration in the software.

Documentation on each newly delivered and deactivated feature is published on the same day the feature is made available online, at the very latest.

Cegid Product teams may decide to deliver, directly in production, long-awaited features, or features that will significantly improve the software's use or functioning. In this case, the documentation is transmitted before it is made available online.

If, for technical reasons, a major feature that impacts the application's ergonomics or operation needs to be delivered directly in production, relevant documentation is transmitted before it is made available online. A reminder is sent out two months before the feature is made available online.

Maintenance Periods

Monday to Friday mornings:	Daily restart 7am
Saturday mornings:	6 am – 8 am CET (with potential production interruption)
Monday evenings:	6:30 pm – 7:30 pm CET (weekly release, with short production interruption to restart the application)

The planned maintenances are communicated on the TS Community, a minimum one week prior to the date, in the section « IT Maintenance and Outages ».

Data Destruction Policy

In case of contract termination or a change in software platform, Cegid agrees to delete all customer data (including the database, URL, and backups). Cegid shall provide customers with a statement of data destruction. Data is deleted 60 to 90 days after the contract is terminated.

Premium Support Comitology

Cegid holds regular committee meetings to maintain Premium support partnerships.

Activity follow-up Meetings

Frequency: Once a semester

Agenda:

- Follow-up on actions carried out since the last meeting
- New actions to be carried out
- Functional questions about the software
- Product developments
- Set deadlines for actions taken during the committee meeting

Participants:

- Cegid: dedicated consultant
- Customer: Central administrator

Steering Committee

Frequency: Twice yearly

Agenda:

- Updates
- Presentation of the work carried out over the period
- KPI review
- Risk management
- Budget management
- Invoicing follow up
- Next steps

Participants:

- Cegid: Dedicated consultant, Customer Success Manager, Account Manager
- Customer: Central administrator

Escalation Process

In case of dispute over an issue, customers can specify in their ticket that they wish to be contacted by Customer Success or a Customer Care manager. A conference call will be scheduled within 5 days of the request being submitted.

Crisis Management Procedure

The objective of the crisis management process is to prevent and lessen the damage of the crisis by triggering an efficient and regular follow-up of actions, which cannot be dealt through standard processes in order to solve the crisis rapidly.

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

The crisis management processes are triggered in the following circumstances:

- In case of force majeure, a blocking incident where a workaround or corrective has not been provided within a reasonable period or prolonged downgraded situations over an unacceptably lengthy period: **ORANGE CODE**
- Widespread blocking incident or degraded situation: **RED CODE**
- All security alerts (known or potential) that jeopardise customer data: **BLACK CODE**

Overview of Crisis Management Process

The first action is to trigger the creation of a crisis unit named « war room ».

The latter identifies the customers that are potentially impacted and establishes a communication plan in order to inform the impacted customers.

In the case of a confirmed Black Code, Cegid's crisis unit is activated and managed by the DPO and ISSM. The unit identifies the customers that may be impacted and communicates with them via representatives who were designated in the project phase as security representatives (ISSM or equivalent).

In other situations (Red Code and Orange Code), the crisis unit includes, but is not limited to, consultant(s) in charge of the incident, Incident manager, Customer Service managers, the Cegid ISSM representative or a member of their team, a Cloud Services representative, and a representative from R&D. The crisis unit works in the same way as for incident management. Thus, regular communication, resolution and post-crisis feedback procedures are all implemented.

The unit is dismantled once the issue is completely resolved, customers informed of the resolution and the incident report created. The incident report is comprised of a summary of the incident, the analysis with root cause, corrective actions and possible preventive measures. Cegid management then carries out an analysis and improvement (if necessary) action plan based on incident teachings.

The crisis management process includes regular communications to Cegid management and executive management when necessary.

Reversibility plan

The contract states that the data stored in the Customer's database belongs to the Customer (see subscription contract). In the event that contractual relations cease, and no later than sixty days from the date on which contractual relations cease, Cegid transfers back to the Customer all data and information received from the Customer as part of the performance of this contract. To enable the Customer to exploit the data in question, the data is transferred back in '.csv' text format without any alteration of the logical structure of this data.

Cegid undertakes to provide the Customer with information on the meaning of columns and links between the data from different files, enabling the Customer to exploit the returned data.

Cegid undertakes to not keep copies of the Customer's data and shall not use the data for any purpose whatsoever.

- Upon reception of the customer's request, a conference call is organised between the Customer Success Manager, the customer or their representative, and the Customer Service. This meeting aims to present the data transfer file format and transfer procedures (SFTP/customer file transfer tool). During this meeting, a data is scheduled for data transfer.
- Once the data transfer date is set, the Customer Service provides the customer with the data transfer files. The customer formally acknowledges receipt of all data. Once received, Cegid shuts down the customer's version of the application and destroys all backups.
- The Customer Service provides the customer with a certificate of destruction.

Request for additional Services

Advanced Services and Talentsoft Academy

The customer may, at any time, issue a request for additional services. This request can be made via a TS Community ticket or via the Customer Success Manager/ Account Manager. Cegid provides the corresponding quote within 15 business days.

For more complex requests, a conference call may be scheduled with the services team before delivering the quote to the customer.

Premium Support

A request for this service can be made by contacting your Sales representative.

Premium Support is a reinforced support service, provided by a team of consultants who are experts on the solution. They master their customer's set-ups and are expert in their attributed customer's context and strategic challenges. The service is structured around 4 axes:

- Facilitate customer's day to day administration by creating a close relationship and regular follow-ups.
- Ensure the customer makes the most of his solution by ensuring the right level of information, training and advice is given.
- Manage the quality of service and the customer's HRIS projects in Run phase by animating committees, advise in the decision-making and action plan monitoring.
- Monitor and scale specific integrations by establishing dedicated technical governance.

HOSTING SITES

Hosting Locations

Cegid currently has several datacentres worldwide in order to grant our clients access to the Cegid Talentsoft application and comply with data-privacy regulations in their native countries.

Geographical area	Country	Primary location (secondary location)	Provider
Europe	France	France Central - Paris (France South - Marseille)	Microsoft Azure France
Europe	Ireland and the Netherlands	North Europe - Dublin (West Europe - Amsterdam)	Microsoft Azure North Europe
Europe	Germany	Germany West Central - Frankfurt (Germany North - Berlin)	Microsoft Azure Germany
Europe	France	Strasbourg (Roubaix/Gravelines)	OVHcloud
North America	Canada	Canada Central - Toronto (Canada East - Quebec City)	Microsoft Azure Canada
Europe **(existing customers only)**	France	Aubervilliers (Saint-Denis / Roissy)	Equinix/Interxion
Europe **(existing customers only)**	Switzerland	Zurich	Interxion
North America **(existing customers only)**	Canada	Beauharnois	OVHcloud
North America **(existing customers only)**	USA	Dallas	IBM SoftLayer
South America **(existing customers only)**	Brazil	São Paulo	IBM SoftLayer
Asia **(existing customers only)**	Singapore	Singapore	IBM SoftLayer

Host Providers Security & Confidentiality

We assess and select our hosting centres according to stringent security, confidentiality, quality, and availability criteria. Having several centres available allows us to be more responsive in setting up new client instances, to share risks and workloads across several suppliers and to increase our capacity rapidly and independently.

Cloud provider and Cegid are bound by a contract that includes a confidentiality clause. The list of people authorised to access the data is reviewed regularly.

Cegid's legal structure is based in France, and Cegid Talentsoft's data centres for European customers are based in the European Union Cegid guarantees that the database is and will always be located in Europe for all European clients. This guarantee also applies to backups.

Therefore, Cegid can guarantee complete protection from the US Patriot Act to all clients who wish to protect themselves against it.

Our hosting centres have the following features in common:

- Data centres designed with high levels of redundancy for extremely high-availability solutions (Tier 3 or equivalent)
- A high-speed communication system built on a network of fully redundant, long-distance fibre optics
- The highest standards of active security
- Ongoing concern for energy efficiency and the minimisation of any environmental impact.

The data centres used by Cegid possess strong certifications, to have more information, please refer to this documentation:

- Microsoft Azure: https://docs.microsoft.com/en-us/compliance/regulatory/offering-home
- Equinix: https://www.equinix.com/data-centers/design/standards-compliance/
- OVH: https://www.ovhcloud.com/en/enterprise/products/hosted-private-cloud/safety-compliance/
- Interxion: https://www.interxion.com/uk/why-interxion/awards-accreditations-memberships
- IBM Softlayer : https://www.ibm.com/cloud/compliance/global

TECHNICAL ARCHITECTURE

The Cegid Talentsoft application is based on a three-tier architecture:

- User workstations use of a web browser and must have internet access
- Application servers respond to https requests
- The data servers are only accessible from the application servers. They host the database search engines as well as client data.

The underlying principles of the Cegid Talentsoft technical architecture allow for:

- Segregation of clients for the purposes of security, confidentiality and availability.
- A high level of customisation of each client environment without impacting other clients, and maintaining the uniformity of the software package at the same time.
- Hosting in data centres which meet Cegid's requirements.

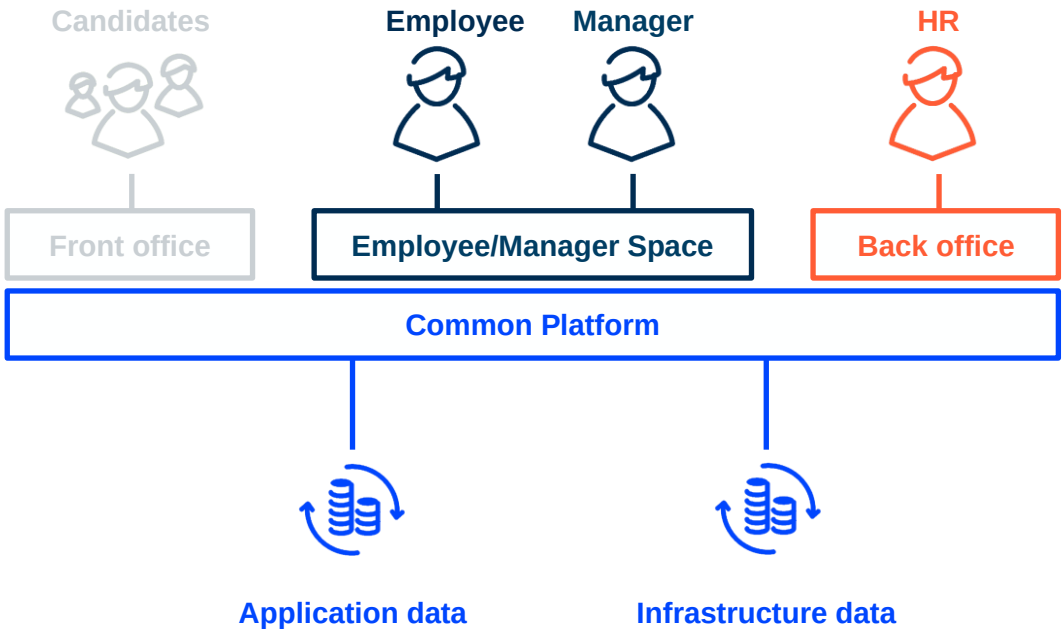
Although Cegid Talentsoft's architecture allows for many options, some of them are not available when using Plug & Play or Adjust & Play project methodologies, also some of them are not available based on the functional scope. These methodologies rely on a short implementation time and reuse of default settings for most aspects of the solution. The native settings of the Plug & Play and Adjust & Play methodologies are described in the commercial offer.

Application Architecture

The Cegid Talentsoft solution is composed of several logic units that are all integrated into one application:

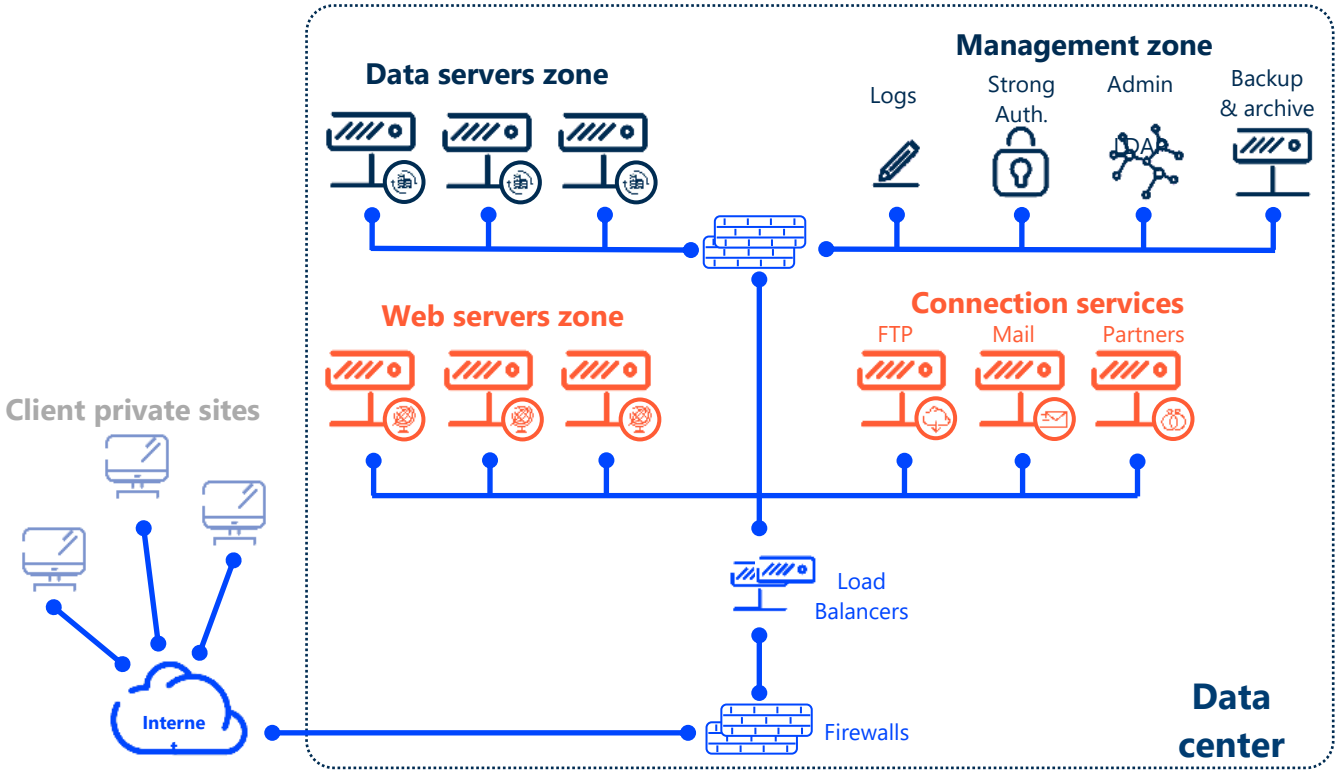
- A personal area. This is the part used by employees and managers. This area makes it possible to access personalized indicators, take action when necessary and to navigate the whole application.
- A back-office. This part is mainly used by HR teams. The back-office is used for all talent-management processes: recruiting, appraisals, mobility, compensation, training, employee reviews, etc. The back-office is sub-divided into two large groups: the talent acquisition back-office, and the talent management back-office.
- One or more front office(s). Front offices enable candidates and employees to view employment vacancies, apply and submit their CVs, manage their applications, and subscribe to mailing lists. It is possible to implement several Front Offices that correspond to several Internet or Intranet portals, each having different functionalities and graphic charters.
- All the information can be constituted within a common database in the Talentsoft Core HR module.

The front office is an independent block as it is exposed to the public internet, and is generally part of a company web site. It can therefore be re-configured and personalized for the client. It is, however, linked to a back-office in order to manage candidates, vacancies and applications.



Server and Network Architecture

Here is a diagram of the architecture implemented for application hosting:



The virtualisation technology used depends on the data centre: VMWare is currently used in our Private Cloud, while our Public Cloud offering is based-off Azure virtual machines.

All the Web servers are provided with advanced load-balancing technology. All database servers are set with synchronous replication using 'Always On Availability Group' features of the Microsoft SQL Server. "Data-Learning" data servers are set to be standalone servers.

The storage and archiving area are physically separated from the production area. The administration area is only accessible by authorised Talentsoft administrators, after a series of 2 firewall filters and a strong authentication sequence. Each administrator uses a named account.

Only web servers have access to data servers, which are therefore inaccessible from the Internet.

Software Technical infrastructure

Infrastructure Components

The employee and candidate management solution was developed on a Microsoft .Net platform. It draws on all of the Microsoft technical architecture: Windows Server Operating System, SQL Server database, IIS application server, C# programming language.

The training design and publication solution (LMS/LCMS) is based on LAMP (Linux/Apache/MySQL/PHP) architecture, as well as a data structure managing training media.

Here is a summary of the main infrastructure components for the current product version:

For .NET modules:

Component	Product	Version
Server operating system	Windows Server	2019
Internet Server	IIS	10.0
Application Framework	.NET	4.8.0
Database engine	SQL Server	2014 SP3 CU4

Concerned: Core HR/HUB, Talent Management, Compensation, Training, Recruiting, Continuous Conversation and Cegid Talentsoft technical departments, Federated identity

For .NetCore modules:

Component	Product	Version
Server operating system	Docker image	1.20 / Alpine 3.1x
Internet Server	Nginx	1.19.x
Application Framework	.NETCore	3.1 & 5
Relational Database engine	SQL Server	2014 SP3 CU4
Non-relational database engine	ElasticSearch	7.16.x

Concerned: AgencyPortal, Talent Match, Talent Profile

For PHP modules:

Component	Product	Version
Server operating system	Linux ubuntu	20.04 LTS
Internet Server	Apache http server	2.4
Application Framework	PHP	7.4
Database engine	MySQL	8

Concerned: LMS, LCMS

Cegid Talentsoft's architecture means different blocks of the above application architecture can be installed on the same physical site or on different sites while also maintaining unity of data and processing. This allows distribution the processing load within the client application beyond the natural load balancing that a shared infrastructure would bring.

Application Databases

A Cegid Talentsoft application is based on a group of databases:

Technical databases that do not contain user data

Database	Usage	Instances
Main-Tenants	Database that lists all 'tenants' in a physical site	One database per data center
Main-Logging	Database that contains the technical logs	A database that can be accessed only by Cegid technical administrators

Databases containing user data

Database	Usage	Instances
Data-Candidates	Database containing mainly data linked to the Talent Acquisition module: the candidate pool, vacancies, applications and their attachments.	One database per client
Data-Employees	Database containing mainly data linked to the following functional modules: Core HR / Hub Talent Management Talent Review Compensation TMS (Training administration)	One database per client
Data-Learning	Database containing mainly data linked to the following modules: LMS (training results) LCMS (training content)	One database per client
Data-OKR	Database containing mainly data linked to the following module: Continuous Conversation (e.g. Key objectives)	One database per data centre with logical client isolation
Data-Sourcing	Database containing mainly data linked to the following module: Hello Talent (e.g. Talent pool)	One database with logical client isolation
Data-File	Datastore containing all attachments (files)	One datastore with logical client isolation
Data-Skills	Database containing all skills definition	A database with logical client isolation

Multi-client Management

The Cegid Talentsoft application is available in the form of web sites. Each client has its own sub-domain which can be served by a unique or shared instance of web server. In this way the product has a multi-tenant software architecture and all the sub-domains point to the latest version of the application. Each tenant has its unique domain (or a few unique domains) that are matched against a unique tenant ID.

Although the product architecture is purely multi-tenant in all cases in the web server (software) layer, multitenancy management in the database layer can vary, with different patterns used depending on the module.

For core databases (Data-Candidates, Data-Employees, Data-Learning) containing most of the individual information, multi-tenancy is very limited as each customer has its own database, co-

hosted on shared SQL servers. In this case, the web server will connect to the tenant database to answer a request. The main reasons for this choice of architecture are:

- Easier management of data security and confidentiality
- Easier backups and restorations.
- Ability to customise the behaviour of each client application instance even though the same product is implemented for all clients

For the Data-OKR, Data-Sourcing, Data-File & Data-Skills databases however, the architecture is different and many customers can share the same database. In this case, the web server will connect to the same database for many clients and the software component responsible for tenant isolation will restrict all requests to the database to the tenant data.

In addition:

- There are no tenant-superseding accounts, meaning that all accounts used to access a module data through the UI needs to be registered in the tenant's databases account management to be used, including service accounts used by Cegid personnel to administrate the environments.
- Tenant data is not encrypted on default, but full encryption of the database can be activated as an additional service. Cegid provides upon request software data encryption of the database.

Reporting/Analytics

All modules share a reporting capability allowing report management, either directly in the user interface or by generating CSV, Excel or PDF files depending on the report. All modules also share an Analytics module which allows the user to explore Cegid Talentsoft HR data through a multi-dimensional cube.

The analytics features are provided through a MS SQL Analysis Services infrastructure. This infrastructure is multi-tenant and each client has their own data cube within a shared MS SQL A.S. engine. Analytics data are kept in the same data centre as operational data. Cegid complies with local data protection regulations in the same way for analytics and operational data.

The Talent Acquisition module also uses Microsoft Reporting Services to manage reports. This product is part of SQL Server. Reports are accessed from the application according to the rights given to the connected user.

Test Environment

Each client is provided with a production URL and a test URL.

Testing environment is installed and managed as an environment that is separated from the production environment. It is managed as if it was the environment of a different client.

Test environments are used to test new functions before they are activated in production, or to test an action. Data in the test environment are a copy of the production data from a given time, and are consequently older.

By default, all data on a testing database are anonymous. If the client makes a support request, Cegid can update the test data using the production data (without attachment and with an appropriate level of anonymization).

Clients may request Cegid not to anonymise data in test environment. However, in this case, clients are responsible for data confidentiality and an extended delivery time is to be expected.

Test environments are not as available as production areas. Furthermore, Cegid reserves the right to interrupt these environments momentarily to carry out various tasks (installations during working hours, for example).

Mobile Application

The Cegid Talentsoft mobile application is available on two mobile platforms: Android and iOS. The application can be downloaded in their respective app stores.

The access to the mobile app can be done either by scanning a QR code or using a manual code. Both codes are shared with the clients' system administrator upon request after activating the mobile application in the client tenant. Single Sign On is supported under the condition that the client has implemented an Identity Provider.

The Cegid Talentsoft Mobile app only provides a presentation layer. This means that no data is stored on the mobile device, except some information such as first name, last name, e-mail address. Personal data are stored in Cegid Talentsoft´s data centres and are accessed in real-time through APIs.

PRODUCTION SERVICES

The implementation of the services below are subject to commercial agreement.

"Dedicated server" Environment

The dedicated server environment is a complete isolation of your data on a dedicated database server.

Additional Environments

Each client has their own production environment and test environment. The test environment is managed as an environment that is completely separated from the production environment.

Other environments can also be added, for example: a second test environment, a training environment, etc.

CDN

For its LMS, Cegid uses a CDN in order to speed up web page and training content load times. This service can be activated on the Cegid Talentsoft LMS on the condition that the standard domain name provided by Cegid is used.

Our supplier, Cloudflare, frequently changes their point of presence (POP) list. The POP list is available on their website : *https://www.cloudflare.com/network/*

Client Site URLs

Each client is provided with a production URL and a test URL.

The client's URL can be personalised. To do this, the client must buy a certificate and redirect his domain name with a CNAME entry using value provided by Cegid. However, if the client customises the domain, this may limit their use of Cegid's CDN service.

This service is free of charge.

Virtual Private Network (VPN)

The applications use the HTTPS protocol as standard.

As a paid option, it is possible to set up a site-to-site IPSec VPN between Cegid Talentsoft and the client.

The VPN associated to a dedicated server environment offers security conditions similar to on-premise hosting, with the benefit of Cegid being responsible for the proper functioning of the infrastructure and for all version updates. Though we recommend our clients who wants a VPN to take both options.

When using the VPN option the Backoffice API cannot be supported.

Data Encryption

By default, only application passwords are encrypted. They are saved in an irreversible manner in the database.

As a free option, Cegid provides a data encryption solution within the SQL Server engine. However, it must be noted that a 5% reduction in performance has been observed.

As a paid option, Cegid can also provide full database encryption with external key vault.

These options do not apply to the LMS, LCMS, Continuous Conversation and Hello Talent modules.

Extended Storage (LxMS only)

The storage allocated by database is 250GB we can provide additional Storage per range of 250Go.

Access Management

Application Access Security

Candidate Front Office

By definition, the Candidate Front Office applications are exposed and accessible via the Internet.

Back Office and Employee/Manager Areas

Several access methods are possible:

- Application exposed and freely accessible via the Internet;
- Application exposed and accessible via the Internet with IP address restrictions;
- Application accessible only via a site-to-site IPSec VPN tunnel between the client network and the Cegid Talentsoft platform (paid option, not included in the standard service). In this case, Cegid's CDN features are not activated
- Access to the application can be limited for specific groups of IP addresses. All accesses outside this defined group of IP addresses will be forbidden.

Authentication

By default, Cegid Talentsoft identification is performed via the entry of a login and password.

Customer Responsibilities

Customers are responsible for their own password policy. However we inform that the following policies may lead to serious privacy law infringement (such as GDPR) :

- Reusing/cloning passwords;
- Use of an algorithm to build the passwords;
- Use of a password known by more than 1 person;
- Use of leaked passwords or "easy to find" passwords such as "Admin1234." Or "AZERty12@";
- Set the complexity under what's recommended by the CNIL : https://www.cnil.fr/sites/default/files/atoms/files/recommandation_passwords_en.pdf

In such cases only the customer would be responsible before the possible incident and his consequences.

Authentication for the Candidate Front Office

Candidates must enter their email address and an associated password (which they must confirm) in order to create a personal space which they can return to later. There is a 'forgotten password' option. The password must contain at least 5 characters.

Authentication in the Employee/Manager Area

Several authentication mechanisms are available for users working with the company.

- Via Cegid Talentsoft login and password
- By Single Sign-on.

It's possible to use several authentication method on the same platform.

The session is fully managed on the server. Only a session cookie is stored on the user workstation and, in certain cases, a view state is contained in the page.

Password Management

Upon the Client's request, Cegid Talentsoft can be configured to implement the following password management policies:

- Change of password at the first connection
- Periodic password renewal, where the period (in days) between renewals can be configured
- Memorisation of the last X passwords to avoid re-use
- Minimum password length of X characters
- Not including MS and LCMS: Account locked after X failed attempts.
- LMS and LCMS: Gradual network degredation after Y-number of failed connection attempts.
- Minimum number of non-alphanumeric, numeric, lowercase and uppercase characters in the password
- Management of account validity end date in the back office
- Password reset via an activation link sent by email
- Forcing email address validation before activating an account
- Prevent use of username text within a password.

There are two types of password policy, one for candidates, the other for employees and solution administrators.

Passwords are secured in the database in a non-reversible way through hashing and salting:

- In HMHMAC-SHA1 for Talent Management
- In PBKDF2 HMAC-SHA1 with 15,000 iterations for Talent Acquisition
- In SHA2-256 for LMS/LCMS

We strongly recommend using SSO if storing passwords on a database poses an issue.

Lost/forgotten passwords. When users forget their password, and are not using SSO, they must do the following:

- Use an Internet browser to access their Cegid Talentsoft login page.
- Enter the login in the 'You have forgotten your password' field, and then click on 'SEND'.
- A re-activation link be sent by email to the user. The user will have to enter a new password before re-connecting to the application.

Single Sign On

If the client has implemented an Identity Provider, then it is possible to authenticate users via Single Sign On based on SAML 2.0, WS Federation, or OpenId Connect protocols. For further details please refer to the public documentation of the SAML 2.0, WS Federation and Open Id Connect protocols.

Cegid Talentsoft supports both "SP initiated SSO" and IdP initiated SSO" modes. The IdP initiated mode is only available with the SAML 2.0 protocol.

Session Duration

A session's duration depends on its particular use in the different Cegid Talentsoft modules:

- A session in the manager/employee portal or back office is halted after two hours of inactivity. The session lasts for a maximum of twelve hours (can be changed with configuration).
- In the Front Office, session duration is 20 minutes.

Cookie Policy

When navigating our applications, cookies are stored on the user's browser. The purpose of the cookies is to collect navigation information, identify the users and allow them access to their accounts.

To get the list of the Cegid Talentsoft cookies, please refer to: https://privacy.talentsoft.com

Regarding cookie-related data, Cegid commits to comply with local regulations in each country, to protect the data confidentiality and to comply with territory obligations regarding data storage location.

Roles, Right & Authorisations

Cegid Talentsoft has a dedicated interface for Roles, Rights & Authorisations administration.

Roles & Rights

Roles are used to define standard profiles with certain access levels to Cegid Talentsoft features. First, the roles are defined; then they are assigned to Cegid Talentsoft users. The rights assigned to the roles are, however, a set list defined within the product. Roles can be completely reconfigured using the TS Administration module in Cegid Talentsoft.

Authorizations

User authorisation lists help define who has the right to access which employee's information. An authorisation list is a list of employees (called "members"). A list is assigned to one or more employees (the owners), who then have access to the members of that list. Authorisations can be completely reconfigured using the TS Administration module in Cegid Talentsoft.

It is possible to generate user authorisation lists automatically from management rules (using an organisation, for example). Such lists are automatically "refreshed". This means that if the content of the organisations changes, then the lists will be automatically updated, usually within a few hours.

INTERFACES

In Cegid Talentsoft, it's possible to import and export data as CSV format files or by using Web Services. This chapter describes the principles behind file and Web Service exchanges as well as the security aspects related to these exchanges. Interface specifications are provided at the beginning of the deployment project.

ImportingExporting Files

Operating Principles

The Cegid Talentsoft solution offers an integrated import/export module. This module enables customers to manually or automatically carry out imports and exports using CSV files. Cegid thereby relies on the Cegid Talentsoft standard interface when exchanging files via other IT solutions.

The operating principles are based on the following points:

- Cegid Talentsoft exposes standard half-interfaces to recover and update data regularly.
- The standard incoming/outgoing interfaces are in CSV format. CSV is a text-based format compatible with all third-party systems that can interface with Cegid Talentsoft.
- Cegid Talentsoft applies the following best practices:

  The format to be used is that of the tool into which the data is imported.
  The client is therefore responsible for ensuring that all half-interfaces comply with the Cegid Talentsoft format.
  Cegid Talentsoft is able to personalise export formats, as long as the format can be expressed in the form of a series of columns in CSV format.

Our vision of integration is based on one simple principle: avoiding double entry. Thus, if data is input in one place, in principle it is only read in the other systems that use it. For example, if Cegid Talentsoft imports administrative data from employees, we start from the principle that this data is read-only in Cegid Talentsoft, even if Cegid Talentsoft offers standard functions that make editing possible.

For a performance and coherent data synchronization, the daily imports must be "differential", i.e. contain only the data which would have changed. And the so-called "Full" imports must be executed on weekends.

Access to each import and each export is controlled by a user access right that is modifiable and administered by the client's HR administrator.

Cegid makes a set of FAQs available to its clients, which sets out good practice for the creation of import files.

List of available Import/Export Formats

Cegid provides over 200 different export/import file formats in CSV for Cegid Talentsoft, thus covering all business objects of the product. Import files must be encoded in **UTF-8 with BOM** to manage international character sets. Cegid provides full documentation on all formats at the beginning of the project.

List of the main objects that can be imported and exported:

- Libraries: values list, resources, translations, mapping tables, etc.
- Employee Core HR: employees, addresses, contact details, contracts, hourly rates, extra fields, etc.
- Organisation data: organisations, key properties, positions, etc.
- Certifications
- Jobs, job families, competencies, etc.
- Training: training requirements, training actions, sessions, registrations, training history, training plans, training costs, LMS content, etc.
- Compensation: salaries, bonuses, advantages, compensation history, salary proposals, etc.
- My Profile: qualifications, experience, training history, etc.
- Appraisals: form fields, training requests, mobility requests, objectives, competencies assessment, salary proposals, etc.
- Candidates: candidates' basic data, qualifications, competencies, jobs, mobility, extra fields, etc.
- Vacancies: Jobs, specialisations, languages, competencies required, vacancy events, extra fields, etc.
- Applications: application events, candidates, etc.
- Training: Trainees, trainers, groups, sessions, registrations, training results, projects, etc.

Secure FTP Interface

The application is designed to exchange data with external systems through interfaces. All file exchanges are authenticated and encrypted (FTPS or SFTP). All web services use HTTPS and require an authentication.

Cegid can automate imports and exports to and from Cegid Talentsoft. The principles behind this automation are the following:

- Each client has a private and secure space on the Cegid ftp site. In this space, the client can place files to be imported or retrieve files that have been exported.
- A scheduler is programmed to carry out imports and exports according to a predefined schedule. Cegid is in charge of configuring the scheduler according to clients' requirements.
- If files are present, they will be processed according to the scheduled instructions. If there are no files, the scheduler does nothing and does not generate any errors.

The scheduler determines the nature and the order of imports to carry out, using the names of the files submitted. Import files must be named according to the following syntax:

```
[ImportType]_[ImportMode]_[Culture]_[Order]_.csv
```

where
`[ImportType]` is the **type** of import to be executed => required field.

The import type corresponds to a type of object to be imported. The possible values for the import type are listed in chapter 0, List of available Import/Export Formats.

`[ImportMode]` is the **mode** of the import to be executed => required field.

List of import modes:

- "InsertOnly"
- "InsertAndUpdate"

[Culture] is the cultural environment code, for example, en-gb format for British English=> non-required field. If the field is not present, the import uses the company's culture setting.

[Order] is an integer corresponding to the (ascending) order of execution of the imports. => Mandatory.

Example of an employee import in 'InsertAndUpdate' mode: importing data in "InsertAndUpdate" mode works as follows: if a row in the import file refers to an existing employee, the fields appearing in the import row are used to update the existing record because the insert/update mode is being used. If there is no row for a particular existing employee in the import file, nothing happens to the employee record. If a line of the import file refers to a non-existing employee, the employee record is created.

Example of an import employee in 'InsertOnly' mode: importing data in 'InsertOnly' mode operates as follows: if a row in the import file refers to an existing employee, the corresponding import row is rejected. If there is no row for a particular existing employee in the import file, nothing happens to the employee record. If a row of the import file refers to a non-existing employee, the employee record is created.

Access to FTP site: Access to Cegid's FTP site is granted through the use of a login and a password, either through FTPS or SFTP (secure) protocol. Cegid renews the password manually at the client's request. Therefore, the password for the FTP site does not expire.

In SFTP, it is also possible to choose to authenticate by exchanging keys in advance. FTPs use passive mode.

Application Programming Interfaces (API)

Cegid provides a number of web services allowing third party applications to use Cegid Talentsoft services. These web services cover the following functional domains:

- Libraries: value list, resources, translations, mapping tables, etc.
- Employee Core HR: employees, addresses, contact details, contracts, hourly rates, extra fields, etc.
- Organisation data: organisations, key properties, etc.
- Appraisals: input and reading of forms
- Candidates: personal information, qualifications, competencies, jobs, mobility, extra fields, etc.
- Vacancies: Jobs, specialisations, languages, competencies required, vacancy events, extra fields, etc.
- Applications: application events, candidates, etc.
- Training: training content publishing management.

Cegid has chosen a REST approach for Web APIs. All calls to the Cegid Talentsoft API are secured through an application key and by a specialised account with its own password.

For the "Training publication management" part, the Web Services protocol is SOAP, secured by IP address or login/password filtering.

By default, one given tenant (i.e. client) can send up to 10,000 API requests per day. Beyond this threshold, you will need to contact your Cegid representative.

The documentation for web services is available on the https://developers.cegid.com/

Email Interface

The Cegid Talentsoft application sends emails using the classic SMTP protocol. Emails can be sent in HTML format, or plain text format whenever clients cannot process HTML emails.

Virtual Classroom Tools: LTI use case

Learning tools interoperability (LTI) is a standard integration method for learning tools, which can be used for a number of learning scenarios. In addition or instead of the tool Moxtra, the tool already integrated into Cegid Talentsoft, also external tools can be used for virtual LMS classes.

There are four different types of tools, which can be used:

- Cegid Talentsoft: for each virtual classroom created, the tool that will be used by default is Moxtra in white label.
- Microsoft Teams: The client can add multiple Microsoft Teams tools if multiple users with different Azure configurations want to use the feature that automatically generates a Teams link.
- Other: other tools can be used to add external video conferencing tools (Jitsi, Skype, etc.). The link to the external virtual classroom tool needs to be added manually.
- LTI1.1: Multiple LTI 1.1 tools can be added. Identified tools are Zoom and Glowbl. The authentication is done via SSO & account provisioning.

Only a super administrator has access to the configuration menu and all the other technical configuration options.

Data Recovery Procedure

This section is completed according to specific client requirements. There cannot be one unique and repeatable approach to this process seeing as transfers involve different data each time.

However, in general:

- Historical data (until an agreed 'cut-off' date agreed on by the client) are imported once. Beyond this date, recurring imports take over.
- We recommend using the standard import/export formats, even for historical data, in order to avoid creating flows that will only be used once.

OPERATIONS

Operating Procedures

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

Purge

Purge of system logs. System logs are kept for 90 days.

Purge of application log. The application log contains the user actions' tracking data. This log keeps one year of data, older data is purged.

Purge of files stored on secure FTP. The files stored on the secure FTP site are kept for maximum 90 days.

Scheduled Tasks (Batch Tasks)

A certain number of batch tasks are provided in the standard application (sending emails, registration for mailing lists, purges, statistical reports, operational actions).

Each task can be initiated with the assistance of an off-the-shelf scheduler that can launch an online command task. Cegid is in charge of managing schedulers.

Specific operating actions. Cegid allows for specific actions to be scheduled in the production and test environment of a client, upon the client's request. However, all requests are subject to approval by Cegid.

Data Back-up

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

Organisation of Backups

Databases backups are performed based on a strategy that involves best data security, integrity as well as time to restore . These are online backups without any service interruption to the database.

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

Action	Backup frequency	Backup retention
Daily Full backup	Once a day	30 days
Monthly backup	Once a month	12 months

The backup media and locations depend on the Cloud provider:

Action	Backup storage	Data replication
Public (Azure)	Azure Blob container	Data is replicated within the same primary location and exported asynchronously to a secondary datacenter
Private (Quadria)	Storage disks	Data is replicated synchronously on a remote datacenter
Private (OVHcloud)	Storage disks	Data is replicated within the same primary location and exported asynchronously to a secondary datacenter

Only a very limited number of people have access to database backups. Such people, like all Cegid personnel, is bound by a confidentiality clause. Likewise, our cloud provider has a limited number of people who are authorised to access backups.

Administration and Supervision

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

A handling and 'escalation' process has been defined and is followed by operational teams.

The tool used for infrastructure supervision is Zabbix. The tool used to monitor application performance is NewRelic. Our host providers also have their own monitoring system.

The operating procedures include the following tasks (non-exhaustive list):

- Administration
- Operating systems maintenance (disk space, logs, etc.)
- Database maintenance
- Tests, qualification and deployment of security updates
- Application maintenance (logs and performance analysis)
- SMTP gateway maintenance

Supervision:

- Application availability monitoring
- Response time monitoring
- Platform load (memory, processors, discs) monitoring
- Network bandwidth monitoring
- Application and system batch task monitoring
- Hardware monitoring

Host providers are responsible for tasks associated with the following elements:

- Physical equipment (server hardware, network equipment, etc.)
- Hypervisors
- Network
- Software updates for operating systems, databases and anti-virus
- Monitoring the above elements
- Verification and qualification of back-ups
- Monitoring and update of anti-virus systems
- Network equipment maintenance

Protection from Malware

Administrators systematically apply all Security patches when they are issued. The application patches are applied after verification by administrators in test environments, in accordance with Cegid Talentsoft's application update policy.

Anti-virus software is used on all servers with automatic updates activated. Antivirus databases are also updated regularly as defined in Cegid Talentsoft's antivirus management policy.

Security tests are carried out every week using Qualys WAS in order to ensure the protection level of the servers.

Management of Technical Vulnerabilities

Developers are sensitised and trained on secure development.

Intrusion tests are carried out every week to test the OWASP TOP 10 using the QualysGuard tool and to ensure the protection level of the application.

Intrusion tests are carried out each year by an external security company.

Business Continuity Plan

Activity Recovery Plan (ARP)

The activity recovery procedures depend upon the datacentre.

- **Azure North Europe**

Customer Data are permanently replicated in a remote datacentre within the same legal area (in the European Union for European clients). Thus, the data from Dublin is replicated in Amsterdam.

Recovery process is based on Data replication and services restauration automation on the remote Azure location

- **Azure Germany:**

Customer Data are permanently replicated in a remote datacentre within the same legal area (in the European Union for European clients). Thus, the data from Frankfurt is replicated in Berlin.

Recovery process is based on Data replication and services restauration automation on the remote Azure location

- **Azure France:**

Customer Data are permanently replicated in a remote datacentre within the same legal area (in the European Union for European clients). Thus, the data from Paris is replicated in Marseille.

Recovery process is based on Data replication and services restauration automation on the remote Azure location

- **Azure Canada:**

Customer Data are permanently replicated in a remote datacentre within the same legal area (in the European Union for European clients). Thus, the data from Toronto is replicated in Quebec City.

Recovery process is based on Data replication and services restauration automation on the remote Azure location

- **Private Cloud France (Quadria/OVHCloud):**

Each database is replicated on a remote datacentre within the same country

Backup storage arrays are replicated asynchronously every 15 minutes towards a remote datacentre within the same country

Recovery process is based activation of the fallback servers in the remote site

- **Private Cloud Switzerland (Quadria):**

Database content is saved and then archived off-site from the production centre.

The recovery plan involves:

Bringing the data centre back online

Restoring the data to the available platforms.

Application Activity Continuity Plan (ACP)

Cegid Talentsoft premises have an Activity Continuity Plan for its application report that can be consulted on-site. The downgraded situations covered by this are:

Downgraded situation	Workaround actions	Private Cloud France (Quadria/OVHCloud) All Public Cloud Azure Locations	Private Cloud Switzerland (Quadria)
Loss of an application server	Operation using other application servers, which take over via load balancing	Impact: • Possible slower response from the application Actions: Restoration of the defective application server. Recovery target: From several minutes to 2 hours	Impact: • Possible slower response from the application Actions: Restoration of the defective application server. Recovery target: From several minutes to 2 hours
Loss of all the application servers	Depending on the severity: Reboot Web virtual machines If the data centre is affected: reboot at another data centre	Impact: • Possible slower response from the application Actions: Depending on the severity, Reboot Web virtual machines Traffic is automatically redirected to second data centre Recovery target: If restarting VMs: From several minutes to 1 hour	Impact: • Total interruption of service Actions: Depending on the severity, Reboot Web virtual machines Recovery target: If restarting VMs: From several minutes to 1 hour If changing data centre: 24 to 72 hours.
Loss of a data server	Depending on the severity: Restart data server virtual machine(s) If the physical servers are affected: Launch of inaccessible databases on a backup data server. The data are 'refreshed' up to the latest observed log shipping.	Impact: • Possible slower response from the application Actions: Automatic redirection of the request to second data server Recovery target: If restarting a VM: several minutes to one hour If restarting on a backup DATA server: several seconds	Impact: Interruption of service for applications with data kept on that server. Actions: Temporary interruption of each application concerned by this server; Modification of the application settings to use another data server; Re-launch of the service for each application impacted Recovery target: If restarting a VM: several minutes to one hour If restarting on a backup DATA server: 1 to 3 hours
Loss of all data servers	Depending on the severity: Restart data server virtual machines	Impact: Interruption of service for applications with their data on that server or interruption of service for all data centre applications. Actions:	Impact: Interruption of service for applications with their data on that server or interruption of service for all data centre applications. Actions: Interruption of all the applications in question;

	If the physical servers are affected: restart in another data centre (web and data). In this case the data will be 'refreshed' up to the most recent daily backup.	Restore Data on another server Recovery target: If restarting a VM: several minutes to one hour If restarting on a backup DATA server: 1 to 4 hours Depending on backup size	Transfer of data to another data centre; Restoration of databases on the data servers Re-launch of the service for each application. Recovery target: • If restarting VM: several minutes to one hour If changing data centre: 24 to 72 hours
Loss of information from a database	Application of the last logs transmitted by the log shipping mechanism If there are restoration issues, search for the data in question in past daily back-ups (up to one month prior) or past monthly back-ups Data restoration	Impact: Interruption of service for the application in question Possible loss of data Actions: • N/A The retrieval of data serves as a return to nominal mode. Recovery target: From several minutes to 1 hour. Possible loss of data if there is a gap between last restored copy and last data updates.	Impact: Interruption of service for the application in question Possible loss of data Actions: • N/A The retrieval of data serves as a return to nominal mode. Recovery target: From several minutes to 1 hour. Possible loss of data if there is a gap between last restored copy and last data updates.
Complete loss of a client database	Restoration of the last back-up made for this client database Application of the last logs by the log shipping mechanism	Impact: • Interruption of service for the application in question • Possible loss of data Actions: N/A The retrieval of data serves as a return to nominal mode. Recovery target: From several minutes to 2 hours Possible loss of data if there is a gap between last restored copy and last data updates.	Impact: • Interruption of service for the application in question • Possible loss of data Actions: N/A The retrieval of data serves as a return to nominal mode. Recovery target: From several minutes to 2 hours Possible loss of data if there is a gap between last restored copy and last data updates.

REGULATION & GUIDELINES

General Data Protection Regulation (GDPR)

Below is a description on how Cegid Talentsoft platform ensures compliance regarding the key requirements of the GDPR.

Important note: all the data security elements are described in the Security Assurance Plan or in other sections of this document; therefore, they are not duplicated here. However, they are all relevant to GDPR in the sense that data security is a key requirement for all subcontractors (i.e. Data Processors).

From the point of view of Cegid Talentsoft, we distinguish between two different personas: candidate and employee. Some of the GDPR requirements do not depend on the personas, and some of them generate different product behaviors depending on whether we address a candidate or an employee.

Coverage of GDPR Requirements applicable to all Personas

Privacy by design

Agile / Software Development process in place includes people training, formal code reviews, and tools to detect application of recommended 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 development of the product.

Privacy by default

Default's level of privacy is always set to the most restrictive level.

Data Protection Officer

Cegid has named a DPO because of the nature of its business.

Processing Register

Cegid maintains a Product processing register for its customers as data processor.

DPAs with Sub-Processors

Cegid delegates part of its activity to subcontractors. DPAs are signed between them and Cegid which contain clauses in compliance with the GDPR.

All ISO 27001 standard procedures are in place. These procedures are part of our information security management system.

Sensitive Data

Talentsoft does not collect sensitive data such as those stated in article 9 of the GDPR. Since Talentsoft offers some flexibility in terms of add-ons to the data model, Talentsoft does not recommend defining extra fields that fall under the definition of 'sensitive data' stated in article 9.

Data breach notification Cegid has a data breach notification procedure. This procedure is defined, maintained, updated and monitored under the ISO27001 ISMS and the GDPR.

In case of data breach involving customer data, Talentsoft commits to notify the customer (i.e. the Controller) as soon as practicable, so that the Customer can themselves comply with the 72 hours deadline with their own data protection bodies.

Automated Decision Process

Cegid does not feature any automated individual decision features, nor any automated profiling feature. All decisions are left to human users that can be helped in their decisions by relevant dashboards, KPIs, recommendations and analytics, whose sole purpose is to help users to make informed decisions.

Data anonymization

Cegid offers a 'full-database' anonymization feature. This is used when a production database needs to be used in either test mode, or debug mode, or training mode.

Information to be provided when personal data are collected from the data subject

It is up to the client to provide this information directly to candidates and employees. Our solution offers the possibility to our customer to provide this information through the configuration of the solution.

Coverage of GDPR Requirements specific to candidates

Candidates are not in a subordinate relationship with the potential employer, who is responsible for the data processing. Therefore, we have clearly stated all possible data processing methods used by the product.

Access rights, rectification rights

Candidates with an account, can access or modify their data from the Front-Office. If candidate doesn't have an account, he can ask the customer's administrator (or DPO) to delete or modify their data by sending them an email. If the customer's administrator (or DPO) needs help, she/he can call Talentsoft Customer Care.

A recruiter can delete or modify a candidate's data if necessary

Candidates can ask for their personal data to be exported. The candidate will then receive an email with a link to download a ZIP file containing all their personal data.

Right to be forgotten

Deletion rights can be automated by entity:

Customers can manage the data retention period by country.
At the end of the retention period, applicants will receive an email asking if they wish to give their consent to the renewal of the retention of their personal data.

If a candidate applies in several countries that have different retention periods, the retention period applied will be the one of the entity linked to the last application action. If the candidate gives his consent to renew the retention of personal data, their data will be saved in the Back Office. If they do not consent, their personal data will be deleted. If they do not answer, data will be deleted after the end of the retention period.

The data deletion is run asynchronously via a scheduled nightly task.

Legal Bases

It's mandatory for the data controller to determine the most appropriate legal basis for the Cegid Talentsoft solution before putting it into production (art. 6.1 of the GDPR).

For information purposes, in order to help determine the legal basis, the CNIL adopted a reference framework " Référentiel relatif aux traitements de données personnelles mise en œuvre aux fins de gestion du personnel " (*Relating to the processing of personal data implemented for personnel management purposes*) on the 21st of November 2019.

In this framework, the CNIL proposes 2 legal bases relating to recruitment:

"**Processing of applications (CV and cover letter) and management of companies**: Pre-contractual measures

-**Constitution of a CV-library**: Legitimate interest".

Any intra-group data transfer must also be justified with a legal basis and made known to the candidates. This information can be provided via Cegid Talentsoft.

Coverage of GDPR Requirements specific to employees

Access rights, rectification rights

The product provides the required features necessary to access and modify employees' data. Access to these features are controlled via roles and rights, which can be attributed directly by the Customers administrators.

Right to request the rectification (and erasure).

Companies have legitimate interests in collecting and processing Employees personal data. In this regard, any data deletion requested by an employee must first be approved by the Employer (i.e. the data controller).

This is why our product offers a delete function in the Cegid Talentsoft Hub user interface. This functionality is subject to a specific right, which can be assigned by the customer's administrators to their concerned users. Currently, the product performs a physical and irreversible deletion of the database.

There are preconditions for deleting the data:

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

The employee's file must be deactivated.

Legal Bases

It's mandatory for the data controller to determine the most appropriate legal basis for the Cegid Talentsoft solution before putting it into production (art. 6.1 of the GDPR).

In the same CNIL Framework cited above ("Référentiel relatif aux traitements de données personnelles mises en œuvre aux fins de gestion du personnel" (*Relating to the processing of personal data implemented for personnel management purposes*) of the 21st of November 2019), the CNIL states, with regard to consent, that: "Employees are only very rarely able to freely give, refuse or revoke their consent, given the dependence that arises from the employer/employee relationship. They can only give their free consent in cases where the acceptance or rejection of a proposal has no consequences for their situation".

Thus, the CNIL proposes other legal bases depending on the activity on employees. A table is available in this framework to help the data controller to determine them.

Web Content Accessibility Guidelines

Cegid is committed to ensuring digital accessibility of its digital services and products in accordance with Article 47 of Act no. 2005-102 of 11 February 2005. Please refer to https://www.cegid.com/en/cegid-talentsoft-accessibility-statement/ for more details.

End of the SOW document, which has 45 pages