cegid

Terms of Services

Cegid Digitalrecruiters

01/04/2024

www.cegid.com

CONTENTS

Modification and Validation History

Original version of the document	1.0	04/08/2023
Revision and updating of the document	2.0	01/04/2024

Audited by

01/04/2024	Alexandre Blanc, Gaëtan Audy & Pauline Hubert Cegid HCM Solution Architect
01/04/2024	Myriam Hétier, Cegid HCM Product Marketing Manager

Approved by

02/04/2024	Stephan Latrille, Digital Recruiters, a Cegid Company CTO

Distribution list

Person or group
Digital Recruiters, a Cegid Company Customer
Digital Recruiters, a Cegid Company, internal

1. INTRODUCTION

1.1. Purpose of the document

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

This document aims to describe the measures taken to ensure the following:

- Quality of support provided by Cegid Digitalrecruiters;
- 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 Digitalrecruiters application for the shared Customer infrastructure.

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

1.2. Modifications to this Document

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

A minor modification will not necessarily result in a new version of the document being issued immediately. Such modifications will be incorporated in the next version of the document.

Any modification to the document becomes part of the document and is equally binding on the parties.

Should the document be modified, the version published on the official Cegid website is the official reference version. The version attached to the customer contract serves to verify that there is no regression as specified in the contract.

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

2. SUPPORT DESCRIPTION

2.1. Support Location

Cegid Digitalrecruiters Customer Care Support teams are based in France (Boulogne-Billancourt), Canada (Montreal), Rijswijk (The Netherlands) and Germany (Cologne). Support requests can be made in English, French, Dutch and German.

Support tickets must be issued via the Zendesk Help centre, a ticketing tool available online from the Cegid Digitalrecruiters application for all Customers with a support contract.

2.2. Support Contract

Cegid Digitalrecruiters provides technical support to Customers for all functional or technical questions, including the following types of support requests in particular: Assistance, Advice, Reporting of Bugs/Anomalies (minor, major, critical).

Technical support is included in the Cegid Digitalrecruiters offer to which the Customer is subscribed. Any other assistance service is subject to a separate contract, based on pricing provided by Cegid Digitalrecruiters.

2.3. Access to Application Resources

The Cegid Digitalrecruiters application Support area offers users a number of resources to help them use the solution. These resources cover the following topic:

- Careers sites;
- Publishing and distributing job postings;
- Managing job applications;
- Configuring settings;
- Managing users;
- Legal and GDPR;
- Back Office;
- FAQs and tips.

2.4. Support Section

Support is available from Monday through Friday, from 9:00 to 18:00 (Paris time), via a ticket management tool within Cegid Digitalrecruiters Solution or, if this option is unavailable, by email at: support@Digitalrecruiters.com.

To ensure effective follow-up, any encountered Bugs must be reported to the Support service in writing using the technical support tool provided (via link) in the Solution. Should the tool be unavailable, the Bug can also be reported directly by email at: support@Digitalrecruiters.com.

The Bug report must describe the context and, where possible, the process for reproducing the Bug. Once sent, a ticket is created automatically in the tracking tool used by the Cegid Digitalrecruiters support team. The ticket will include the information submitted by the Solution user along with the date and time of the report.

Once the Bug report is received, the support team will assign a level of urgency based on the levels defined in section 2.6 of this document.

The following process is then applied to resolve the Bug:

- Customer Care Operator analyses the bug or request and reproduces it if applicable;
- For technical bugs, Customer Care Operator escalates the ticket to the Cegid Digitalrecruiters product team;
- Product team creates a Jira ticket linked to the Zendesk ticket;
- Cegid Digitalrecruiters develops a patch;
- Cegid Digitalrecruiters project manager tests patch in the development environment;
- Cegid Digitalrecruiters project manager tests patch in the pre-production environment;
- Cegid Digitalrecruiters uploads patch to the production (live) environment.

2.5. Support Ticket Workflow between Customer and Cegid

The following table explains the different Zendesk (ticket management tool) statuses with the corresponding prime (assigned actor) for each status.

Status	Definition	Prime
New	The ticket is created by the Customer and sent to Cegid. This status is automatically assigned by Zendesk when the ticket is created.	*Cegid*
Open	The ticket is being processed by Cegid. This status is assigned by Zendesk once a Customer Care Operator has analysed the ticket and provided an initial qualified response to the customer.	*Cegid*
Pending	The ticket has been qualified by the Customer Care Operator but requires additional information or validation by the customer. The ticket is pending a response from the customer. Pending tickets remain in this status for 5 days before changing to resolved if no response is received.	*Customer*
Resolved	A response has been provided to the customer; the problem is considered resolved. The ticket can be re-opened by the customer. Resolved tickets remain in this status for 2 days before changing to closed if no response is received.	*Customer / Cegid*
Closed	The ticket is closed and cannot be re-opened. A follow-up ticket can be created.	Cegid

2.6. Contractual Definition of Bugs and SLA Policy

2.6.1. Definitions

A Bug is defined as a malfunction which can be attributed entirely or in part to the Solution. There are three levels of Bugs:

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 anomaly:

- 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 anomaly:

- 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.

2.6.2. Cegid Standard SLA for Cegid Digitalrecruiters

Bug resolution time

The bug resolution times are as follows:

- Critical: within a maximum of 1 business day;
- Major: within a maximum of 2 business days;
- Minor: within 30 business days or during a forthcoming minor update of the application, depending on the type of bug.

Cegid Digitalrecruiters cannot be held responsible for Bug resolution times being exceeded in the following circumstances:

- Refusal of the Customer to collaborate in the resolution of bugs, and in particular to answer questions and requests for information;
- Use of the Solution for a purpose for which it is not intended, or in a manner not compliant with its documentation;
- Unauthorised modification of the Solution by the Customer;
- Failure by the Customer to fulfil their obligations with regard to the Contract;
- Use of any package, software or operating system not compatible with the Solution;
- Bug resulting from incorrect operation related to a Third Party or Partner solution.

2.6.3. SaaS Availability

The monthly availability rate of the Solution is 99.5% (ninety-nine point five percent), 24 hours a day, 7 days a week. Availability is calculated excluding the maintenance period.

The availability of the Service is measured based on monitoring by a third-party company. Service availability tests are performed every minute from different sources on the internet located on different internet operator networks.

The monthly downtime (DT) is calculated as follows:

DT (minutes) = Total downtime of the Service in minutes during the month

The overall monthly available time (AT) is calculated as follows:

AT (%) = [1- (DT / (no. of days in the month * 1,440))] x 100

Availability statistics will be made available to the Customer upon request.

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	Actor	Action
1	Customer	Create request
2	Level 1 - Customer Care	File request / Gather additional information
3	Level 1 - Customer Care	Assess complexity
4	Level 2 - Technical support	Conduct technical analysis
5	Level 3 - R&D	Implement corrective action
6	Level 1 - Customer Care	Confirm resolution of request

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	Cegid Customer Care Level 2	Level 3: Product/Technical Support/Production	Customer Care Manager/Customer Success Manager
Submitting support requests	R, A	I, C			
Processing support requests	C, I	R, A	C	C	C
Validating support request resolution	R, A	I			
Crisis management	C, I	R	C	C	R, A

3.1.2. Support Service Quality Control

The following quality control measures are in place to ensure the quality of support service:

- Weekly review of indicators by Customer Care management, with improvement plans and action monitoring;
- Review of immediate Customer evaluations and improvement plans;

- Daily review of ticket queues;
- Preventive alert rules in case of potential Customer escalation or breach of the SLA identified in the ticket management tool.

3.2. Change Management Procedure

3.2.1. Version Management

Cegid Digitalrecruiters conducts daily upgrades to the Solution version, including the implementation of patches and new features.

All development is tested; and a thorough qualification process is conducted for each new version in a pre-production environment before roll-out in the production environment.

Cegid Digitalrecruiters conducts a series of automated tests which must be successfully completed before a new version can be rolled out in production.

3.2.2. Maintenance Periods

Cegid Digitalrecruiters agrees, as part of the Contract, to ensure the maintenance of the Solution throughout the duration of the Contract. As such, it agrees to perform, at its own expense, any intervention or repair necessary to keep the Solution in perfect working order.

Maintenance operations resulting in an interruption to services or degraded performance shall be carried out:

- Without prior notice if absolutely necessary
- With 7 days' notice for any intervention likely to exceed 30 (thirty) minutes.

3.3. Crisis Management Procedure

The objective of the crisis management procedure is to prevent and mitigate any damage caused by a 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, as well as security alerts. The procedure includes an escalation process that can escalate the incident to Cegid's executive management. The crisis management procedure is organised around a single interface created by the Customer Service team.

The crisis management procedure is triggered under the following circumstances:

- In cases of force majeure, of critical incidents for which a workaround or patch has not been provided within a reasonable period of time, or of diminished solution performance lasting an unacceptable period of time;
- Generalised blocking incidents or diminished solution performance;
- All security alerts (known or potential) that endanger Customer data;

3.4. Contract Termination

3.4.1. Reversibility Plan

The contract stipulates that data stored in the Customer's database belongs to the Customer (see the subscription contract). In the event of termination of the contractual relationship, the Customer must therefore, before the last day of the Service, recover their data accessible through the features of the Service, or request from Cegid the return of their Data. Cegid sends the Customer all data and information received from the Customer as part of the execution of this contract. To enable the Customer to use the data in question, it is sent in a standard market format described by the reversibility procedure.

Cegid Digitalrecruiters agrees not to retain copies of the Customer's data and not to use the data for any purpose whatsoever.

3.4.2. Data Destruction Policy

In the event of termination of the contract or a change of software platform, Cegid agrees 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 3 months after the end of the contract.

4. HOSTING SITES

4.1. Hosting Locations

Cegid Digitalrecruiters currently has several data centers across the European Union.

Geographical Area	Country	Main Location	Service Provider
European Union	France	Roubaix (Strasbourg/ Gravelines)	OVHcloud

4.2. Security and Confidentiality of Hosting Service Providers

We assess and select our hosting centres based on strict criteria of security, confidentiality, quality and availability.

The Cloud provider and Cegid Digitalrecruiters are bound by a contract that includes a confidentiality clause.

The legal structure of Cegid Digitalrecruiters is based in France and the data centres for our Customers are based in the European Union (including France). Cegid Digitalrecruiters guarantees that solution data will always be located in European Union for all European Customers. This guarantee also applies to backups.

Our hosting centres have the following features in common:

- Data centres designed with high levels of redundancy for high-availability solutions (tier III or equivalent);
- High-speed communication system based on a fully redundant long-distance fibre optic network;
- Highest standards of active security;
- Constant focus on energy efficiency and desire to limit any environmental impacts.

The data centres used by Cegid hold leading industry certifications: https://www.ovhcloud.com/en-gb/enterprise/certification-conformity/

5. TECHNICAL ARCHITECTURE

The Cegid Digitalrecruiters 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. They host the database search engines, as well as the Customer data.

The underlying principles of Cegid Digitalrecruiters' technical architecture allow for:

- The logical separation of Customers for security, confidentiality and availability purposes;
- A high level of customisation of each Customer's environment, without impacting other Customers, while maintaining the uniformity of the software package;
- Hosting in data centres that meet Cegid Digitalrecruiters' requirements.

5.1. Application Architecture

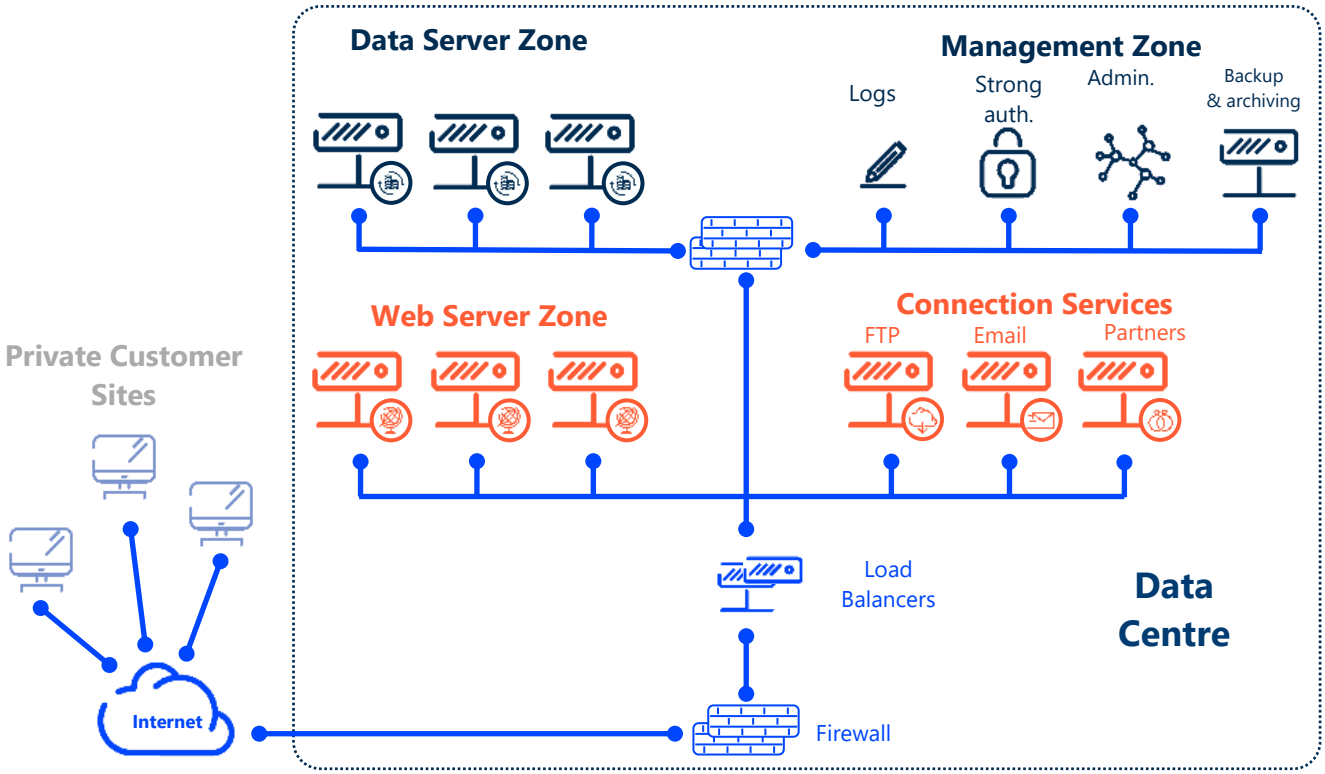
The Cegid Digitalrecruiters solution consists of several logical units, all integrated into a single application:

- Back Office (ATS). This area is mainly used by HR teams and managers. The Back Office is used for all recruitment processes.
- Front Offices (Career Sites). Front Offices allow candidates and employees (via internal mobility sites) to view job vacancies, apply and submit their CVs, and sign up for mailing lists. It is possible to run multiple Front Offices corresponding to multiple internet or Intranet portals, each having different features and graphic charters.
- All information can be contained in a shared database.

The Front Office is an independent block, since it is exposed to the public internet, and generally forms part of a company website. As such, it can be reconfigured and customised for the Customer. It is also linked to a Back Office in order to manage candidates, job vacancies and applications.

5.2. Server and Network Architecture

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



The virtualisation technology used is VMware.

All Web servers are equipped with advanced load balancing technology. All database servers are configured with synchronous replication.

The storage and archiving zone is physically separate from the production zone. The administration zone is only accessible to authorised Cegid Digitalrecruiters administrators, following a connection via a jump server and a strong authentication sequence. Each administrator uses a named account.

Only the Web servers have access to the data servers, which cannot therefore be accessed from the internet.

5.3. Technical Software Infrastructure

5.3.1. Infrastructure Components

The Cegid Digitalrecruiters solution has been developed based on the following technical architecture:

- Linux operating system
- MySQL Server database
- Nginx application server
- PHP programming language.

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

Component	Product	Version
Server operating system	Linux Debian	10 & 11
Internet server	Nginx	
Database engine	MySQL	5.7
Non-relational database engine	ElasticSearch	7.4
Cache engine	Redis	5.7.0.7
Queuing engine	RabbitMQ	3.11.5

5.3.2. Application Databases

A Cegid Digitalrecruiters application is based on a cluster of multi-tenant databases containing technical data (configuration, operations, etc.) and Customer data (pool of candidates, job vacancies, applications, etc.).

Customer data is separated logically and is encrypted when at rest.

5.4. Multi-Customer Management

The Cegid Digitalrecruiters application is available in the form of websites. For the Front Office area, each Customer has its own sub-domain, served by a single instance of the Web server. The product has a multi-tenant software architecture, and all sub-domains point to the latest version of the application.

5.5. Test Environment

Depending on the contractual terms, Customers can have access to a test environment.

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 an action or a configuration, or for training purposes. The data in the test environment can be a copy of the production data from a given time and, in such cases, is therefore older.

Test environments typically have lower availability rates than production environments. In addition, Cegid Digitalrecruiters reserves the right to temporarily interrupt these environments to perform various tasks (for example installations during working hours).

5.6. Mobile App

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

Unique authentication is supported as long as the customer has an identity provider in place.

The Cegid Digitalrecruiters mobile app only provides a presentation layer. This means that no data is stored on the mobile device. Personal data is stored in the Cegid Digitalrecruiters data centres and can be accessed in real time via APIs.

6. ACCESS MANAGEMENT

6.1. Application Access Security

6.1.1. Candidate Front Office

By definition, the Candidate Front Office component of the solution is available and accessible via the internet.

6.1.2. Back Office and Employee/Manager Spaces

The Back Office component is available and freely accessible via the internet;

6.2. Authentication

The platform access control policy can be:

- Managed via the Digitalrecruiters application: entering a login and password.
- Delegated to our customers for the activation of a single sign-on mechanism (SSO), in which case the customer's policy applies.

6.2.1. Customer Responsibilities

If authentication is delegated, Customers are responsible for their own password policy otherwise it will be managed by Cegid Digitalrecruiters Password Management (6.2.4).

6.2.2. Authentication for the Candidate Front Office

Front Office access is not subject to authentication.

6.2.3. Authentication in Back Office

The following authentication mechanisms are available for customer Users:

- Using the Cegid Digitalrecruiters login and password
- Using the single sign-on (SSO) implemented by the Customer.

The session is managed entirely on the server. Only a session cookie is stored on the User's workstation, and, in certain cases, the page contains a view status.

6.2.4. Password Management

Cegid Digitalrecruiters enforces the following password management policies:

- Change of password on first login;
- Minimum password length of 12 characters;
- Minimum number of non-alphanumeric, numeric, lower case, upper case and special characters in the password;
- Password reset using an activation link sent by email;
- Mandatory validation of email address before activating an account;

Passwords are irreversibly secured in the database using the Bcrypt algorithm.

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

- Use an internet browser to access their Cegid Digitalrecruiters login page;
- Click the "Forgot your password" field, enter their email address, then click "CONFIRM";
- The User will receive a reactivation link by email. The User must enter a new password before logging back into the application.

6.2.5. Single Sign-On

If the Customer has an identity provider in place, then Users can be authenticated via single sign-on based on SAML 2.0 protocols.

6.2.6. Session Duration

A session in the Back Office portal is interrupted after eight hours of inactivity. A session lasts for maximum twenty hours.

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, identify Users and allow them to access their accounts.

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

The processing of cookies is described at the following location:

https://www.Digitalrecruiters.com/en/privacy-policy

6.4. Roles, Rights and Accreditations

Cegid Digitalrecruiters 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 Digitalrecruiters features. Roles are first defined and then assigned to Cegid Digitalrecruiters Users. The rights assigned to roles are also configurable within the product. Roles can be fully reconfigured using the rights management module.

6.4.2. Accreditations

User accreditation lists allow you to define who has the right to access the information of a given resource.

7. INTERFACES

In Cegid Digitalrecruiters, data can be imported and exported in the form of files in CSV format or by using Web Services.This section describes the underlying principles behind file exchanges and Web Services, 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. Import

The Cegid Digitalrecruiters solution allows imports using CSV files for the following features:

- Import of applications;
- Import of organisational tree structure;
- Import of users;

The implementation of these imports is described in full in dedicated documents and is arranged with Cegid Digitalrecruiters teams when rolling out the solution.

7.1.2. Export

The Cegid Digitalrecruiters solution allows exports to CSV files for the following data:

- Organisational tree structure;
- Statistics.

7.2. Secure FTP Interface

If required, the implementation of a customer file exchange platform will be arranged with Cegid Digitalrecruiters teams when rolling out the solution.

7.3. Application Programming Interfaces (API)

Cegid provides a certain number of Web Services allowing third party applications to use Cegid Digitalrecruiters services. These Web Services cover the following functional domains:

- Export of recruited candidate applications;
- Addition of adverts to the careers site;
- Export of job postings;
- Number of job postings per department;
- Modification of job postings;
- Import of applications;
- Export of applications.

The implementation of these APIs is described in full in dedicated documents and is arranged with Cegid Digitalrecruiters teams when rolling out the solution.

7.4. Email Interface

The Cegid Digitalrecruiters application sends emails using the standard SMTP protocol. Emails can be sent in HTML format.

8. OPERATIONS

8.1. Operating Procedures

This section describes the most used operating procedures during the service.

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

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

8.2. Data Management

8.2.1. Data Backup

This section applies to production data.

Organisation of Backups

Backups of the different types of data are performed based on a strategy that optimises data integrity and security, as well as restoration time. Backups are conducted online without any interruption of the database service.

Data	Action	Frequency	Conservation
Database	Complete backup	Every 24 hours	30 days
Database	Partial backup	Every 2 hours	24 hours
NAS	Full replication	Once a day	-
Logs	Complete backup	Once a day	3 months

The backup media and locations depend on the Cloud provider:

	Backup Storage	Data Replication
OVHcloud	Object Storage	There is native replication of encrypted data by the Object Storage service in different geographical areas.

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 authorised to access backups.

8.2.2. Data Encryption

Encryption of Data in Transit

To ensure the security of data in transit, Cegid encrypts the application flow with the HTTPS protocol for all domains and requires Transport Layer Security (TLS) protocol 1.2 or higher.

Encryption of Data at Rest

Passwords are irreversibly secured in the database using the Bcrypt algorithm. Cegid provides AES-XTS encryption of volumes.

8.3. Administration and Supervision

The platform is supervised 24 hours a day, 7 days a week. Performance monitoring and application supervision are in place and will trigger alerts if issues are detected. A processing and escalation procedure has been defined and is followed by the operational teams.

The tools used for supervision of the infrastructures are Splunk Observability and Centreon. Our hosting providers also have their own surveillance system.

Operating procedures include, but are not limited to, the following tasks:

- Administration;
- Maintenance of operating systems (disk space, logs, etc.);
- Database maintenance;
- Tests, qualification and rollout of security updates;
- Application maintenance (logs and performance analysis);

Supervision:

- Monitoring of application availability;
- Monitoring of response time;
- Monitoring of the platform load (memory, processors, drives);
- Monitoring of the network bandwidth;
- Monitoring of batch tasks for applications and systems;
- Monitoring of hardware.

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

- Physical equipment (server hardware, network equipment, etc.);
- Hypervisors;
- Network;
- Software updates for operating systems, databases and antivirus software;
- Monitoring of the above;
- Verification and qualification of backups;
- Monitoring and updating of antivirus systems;
- Maintenance of network equipment.

8.4. Business Continuity Plan

A high-availability production infrastructure is in place, based on a division of the services, with each service ensured by a cluster of independent servers, guaranteeing the resilience of the infrastructure. Should one machine (or several machines simultaneously) malfunction, the other servers of the cluster will temporarily absorb the additional workload, ensuring continuity of the service.

This organisation also offers a scalable infrastructure with the ability to easily increase capacity by deploying new machines as needed. For maximum efficiency, the Ansible and Terraform tools are used to automate the deployment and configuration of additional machines.

All measures to ensure the continuity of activity of the Cegid Digitalrecruiters service are described in the document Continuity and Disaster Recovery Plan.

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 Digitalrecruiters.

Important: all data security elements are described in the Security Assurance Plan or in other sections of this document; they are not therefore 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 Digitalrecruiters, as a data processor, distinguishes between two different personas: candidates and employees. Some of the requirements of the GDPR are not dependent on personas, and some of them result in different product behaviour depending on whether addressed to a candidate 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.

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 in its capacity as a data processor.

DPAs with subsequent data processors

Cegid delegates part of its activity to subcontractors. Cegid signs DPAs with these subcontractors, containing clauses compliant with the GDPR.

Sensitive data

Cegid Digitalrecruiters does not collect sensitive data, such as that mentioned in article 9 of the GDPR. As Cegid Digitalrecruiters offers a certain flexibility in the add-ons 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.

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 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 Digitalrecruiters 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 analyses to make an informed decision.

Data anonymisation

Cegid Digitalrecruiters offers a "complete database" anonymisation 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 its candidates and employees. Our solution offers our customers the ability to provide this information, via a configuration.

9.1.2. Response to the GDPR Requirements on Candidates

Candidates have no hierarchical relationship with the potential employer who is the data controller. For this reason, we have defined all possible data processing methods used by the product.

Right of access, right of rectification

Candidates can send an email to the customer administrator (or DPO of the data controller) to request the deletion or rectification of their personal data. The customer administrator (or DPO) can contact the Cegid customer service teams for assistance. A recruiter can also delete or rectify a candidate's personal data if necessary.

Right to be forgotten

The rights of deletion can be automated by organisational unit:

- This allows customers to manage data retention periods by country.
- At the end of the retention period, candidates will receive an email asking them if they want to give consent to extend the retention of their personal data.
- If a candidate submits job applications in several countries with different data retention periods, the applicable retention period will be that of the organisation involved in the last application action. If the candidate gives their consent to extend the retention of their personal data, their personal data will be stored in the back office. If the candidate does not

give their consent, their personal data will be deleted. If the candidate does not reply, their personal data will be deleted at the end of the data retention period.

Personal data is deleted asynchronously during scheduled night-time procedures.

When a request to exercise the right to be forgotten is directly submitted to the data controller, the latter must process the anonymization of the applications that have been made on its job offers and the possible registration for the email alert newsletter. To do this the cutomers must:

- Anonymize applications using the Cegid Digitalrecruiters solution;
- Make a request to delete your newsletter subscription to Cegid Digitalrecruiters support.

Legal basis

The data controller is required to determine the most appropriate legal basis for their context (art. 6.1 of the GDPR) before the Cegid Digitalrecruiters solution goes into production.

For information purposes, in order to help to determine the legal bases, the French data protection authority (CNIL) adopted a reference document "*on the processing of personal data used for personnel management*" on 21 November 2019.

In this reference document, the CNIL suggests 2 legal bases relating to recruitment:

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

-***Creation of a CV library**: Legitimate interest*"

Any intra-group data transfer must also be justified with a legal basis and brought to the attention of the candidates.

9.1.3. Response to the GDPR Requirements on Employees

Right of access, right of rectification

The product provides the necessary features to access and modify employees' 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. Any request to delete personal data made by an employee must be approved by the employer (the data controller).

For this reason, our product offers a deletion function in the Cegid Digitalrecruiters user interface. This feature is subject to a specific right, which can be assigned by customer administrators to the users concerned. Currently, the product physically and irreversibly deletes the database.

Legal basis

The data controller is required to determine the most appropriate legal basis for their context (art. 6.1 of the GDPR) before the Cegid Digitalrecruiters solution goes into production.

In the same CNIL reference document cited above ("*Référentiel relatif aux traitements de données personnelles mise en œuvre aux fins de gestion du personnel*" (Reference document on the processing of personal data used for personnel management) of 21 November 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 for employees depending on the activity. This document contains a table to help the data controller to determine these legal bases.