cegid

Cegid Digitalrecruiters

Livret de Services

16/08/2023

www.cegid.com

SOMMAIRE

Historique des Modifications et des Validations

Création du document	01	04/08/2023

Auditeur(s)

12/08/2023	Alexandre Blanc, architecte solutions Cegid HCM
12/08/2023	Myriam Hétier, Product Marketing Manager Cegid HCM

Approbateur(s)

16/08/2023	Stephan Latrille, CTO Digital Recruiters a Cegid Company

Liste de distribution

Personne ou groupe
Client Digital Recruiters a Cegid Company
Interne Digital Recruiters a Cegid Company

1. INTRODUCTION

1.1. Objet du Livret de Services

Le livret de service fait partie intégrante du contrat et explique les dispositions particulières applicables aux services Cegid Digitalrecruiters.

Ce document vise à décrire les mesures prises pour assurer les éléments suivants :

- qualité du support fournie par Cegid Digitalrecruiters ;
- qualité des processus de suivi et d'escalade des demandes pendant la phase RUN post-projet (phase Build) ;
- RACI du support ;
- description de l'architecture technique de l'application Cegid Digitalrecruiters, pour l'infrastructure Client partagée.

Ce document est mis à jour à chaque évolution de l'environnement technique du service.

1.2. Evolution du Document

Toute évolution de ce document fait l'objet d'une nouvelle version du présent document. Les modifications sont enregistrées et datées dans l'historique des versions placé en début de document.

Une modification mineure n'entraînera pas nécessairement de nouvelle version immédiate du document. Cette modification sera intégrée dans la prochaine version.

Toute évolution du document fait obligatoirement partie de celui-ci et engage les parties au même titre.

En cas d'évolution du document, la version publiée sur le site officiel de Cegid fait référence. La version annexée au contrat client permet de vérifier qu'il n'y a pas de régression telle que prévue au contrat.

Ce document est révisé à minima annuellement. Cette révision peut donner lieu à l'édition d'une nouvelle version.

2. DESCRIPTION DU SUPPORT

2.1. Localisation des Équipes de Support

Les équipes de support Customer Care de Cegid Digitalrecruiters sont basées en France (Boulogne-Billancourt), au Canada (Montréal), à Rijswijk (Pays-Bas) et en Allemagne (Cologne). Les demandes de support peuvent être faites en anglais, français, néerlandais et allemand.

Les tickets de support doivent être émis via le Centre d'aide Zendesk, un outil de ticketing disponible via Internet depuis l'application Cegid Digitalrecruiters pour tous les Clients ayant un contrat de support.

2.2. Contrat de Support

Cegid Digitalrecruiters assure un support technique au Client pour prendre en charge les questions d'ordre fonctionnel ou technique, incluant notamment les demandes de natures suivantes : Assistance, conseil, déclaration d'Anomalie (mineure, majeure, bloquante)

Le support technique est inclus dans l'offre de Cegid Digitalrecruiters souscrite par le Client. Toute autre prestation d'assistance devra faire l'objet d'un contrat distinct, sur la base d'un devis établi par Cegid Digitalrecruiters.

2.3. Accès aux Ressources Applicatives

L'espace de Support de l'application Cegid Digitalrecuriters offre aux utilisateurs de nombreux articles susceptibles de les aider dans l'utilisation de la solution sur les thèmes suivants :

- Sites Carrières ;
- Publication et diffusion d'annonces ;
- Gestion des candidatures ;
- Paramétrages ;
- Gestion des utilisateurs ;
- Légal et RGPD ;
- Back Office ;
- Questions diverses et astuces.

2.4. Section Support

Le support est disponible du lundi au vendredi de 9h00 à 18h00, heure de Paris, via un outil de gestion de tickets mis à disposition par Cegid Digitalrecruiters au sein de la Solution ou, en cas de dysfonctionnement, par email (support@Digitalrecruiters.com).

Afin d'être suivi de manière efficace, une Anomalie constatée doit impérativement être déclarée au Support par écrit via l'outil de support technique mis à disposition au sein de la Solution. En cas de non-accessibilité de l'outil, l'Anomalie peut également être envoyée directement par email à support@Digitalrecruiters.com.

La déclaration de l'Anomalie devra décrire le contexte et, sauf impossibilité, le processus de reproduction. Une fois envoyé, un ticket est automatiquement créé dans l'outil de suivi utilisé par l'équipe support de Cegid Digitalrecruiters. Le ticket intégrera alors les informations de l'Utilisateur de la Solution ainsi que la date et l'heure de la déclaration.

Une fois la déclaration de l'Anomalie reçue, l'équipe support attribue un niveau de criticité selon les niveaux définis au paragraphe 2.6.

Le processus suivant est alors mis en œuvre pour résoudre l'Anomalie :

- Analyse de la demande ou anomalie et reproduction le cas échéant ;
- En cas d'anomalie technique, escalade du ticket par le *Customer Care Operator* à l'équipe produit Cegid Digitalrecruiters
- Création d'un ticket Jira par l'équipe produit associé au ticket Zendesk
- Développement du correctif par Cegid Digitalrecruiters;
- Tests sur un environnement de développement par un chef de projet Cegid Digitalrecruiters;
- Tests sur un environnement de *staging* par un chef de projet Cegid Digitalrecruiters;
- Mise en ligne du correctif par Cegid Digitalrecruiters;

2.5. Workflow des Tickets entre le Client et Cegid

Le tableau ci-dessous explique les différents statuts Zendesk (outil de gestion de tickets) avec le demandeur correspondant pour la progression du ticket.

Statut	Définition	Responsable
Nouveau	Le ticket est créé par le Client et envoyé à Cegid. Ce statut est automatiquement mis à jour par Zendesk lors de la création du ticket.	*Cegid*
Ouvert	Le ticket est en cours de traitement par Cegid. Ce statut est mis à jour par Zendesk dès qu'un Customer Care Operator a analysé le ticket et fait une première réponse qualifiée au client.	*Cegid*
En attente	Le ticket a été qualifié par le *Customer Care Operator* mais nécessite des informations complémentaires ou une validation du client. Le ticket est en attente du retour du client. Ticket en attente reste 5 jours sur ce statut avant de passer en résolu si aucun retour	*Client*
Résolu	Une réponse a été apportée au client, le problème est considéré comme résolu. Le ticket peut être ré ouvert par le client. Un ticket résolu reste 2 jours sur ce statut avant de passer en clos si aucun retour	*Client/Cegid*
Clôturé	Le ticket est fermé et ne peux pas être réouvert. Il est possible de créer un ticket de suivi.	Cegid

2.6. Définition Contractuelle des Anomalies et Politique de SLA

2.6.1. Définitions

Une Anomalie est définie comme un dysfonctionnement, imputable à tout ou partie de la Solution. Il existe trois niveaux d'Anomalies :

Anomalie bloquante :

- Dysfonctionnements rendant impossible l'exécution de tâches essentielles, entraînant une interruption des activités RH.
- Dysfonctionnements qui ne disposent d'aucun moyen de contournement.
- Interruptions dans les tests de fonctionnalités et, plus précisément, les anomalies qui :
    - Altèrent les données ou leur cohérence.
    - Bloquent le flux des processus métier.
    - Produisent des résultats inexploitables pour les processus métier.

Anomalies majeures :

- Dysfonctionnements rendant impossible l'exécution d'une tâche, mais pour lesquels des solutions de contournement existent :
    - Le système peut être utilisé, mais avec une qualité de fonctionnement réduite.
    - L'anomalie perturbe l'exécution de l'action, mais n'empêche pas les Utilisateurs de pouvoir tester les autres fonctions.

Anomalies mineures :

- Dysfonctionnements pour lesquels il existe des solutions de contournement et qui n'ont pas d'incidence sur d'autres fonctionnalités :
    - L'impact sur l'utilisation de l'application est insignifiant.
    - Exemples : anomalies qui modifient l'ergonomie du système.

2.6.2. SLA Standard Cegid pour Cegid Digitalrecruiters

Temps de résolution des anomalies

Les délais de résolution d'Anomalie sont les suivants :

- Anomalie bloquante : sous 1 jour ouvré maximum ;
- Anomalie majeure : sous 2 jours ouvrés maximum ;
- Anomalie mineure : sous 30 jours ouvrés ou durant une prochaine mise à jour mineure de l'application selon la typologie de l'anomalie.

Cegid Digitalrecruiters ne peut être tenu responsable du dépassement d'un délai de résolution d'Anomalie dans les cas suivants :

- Refus du Client de collaborer dans la résolution des anomalies et notamment de répondre aux questions et demandes de renseignement ;
- Utilisation de la Solution de manière non conforme à leur destination ou à leur documentation ;
- Modification non autorisée de la Solution par le Client ;
- Manquement du Client à ses obligations au titre du Contrat ;
- Utilisation de tout progiciel, logiciel ou système d'exploitation non compatible avec la Solution.
- Anomalie résultant d'un mauvais fonctionnement lié à une solution de Tiers ou de Partenaire.

2.6.3. Disponibilité du SaaS

La Solution est disponible mensuellement à 99,5 % % (quatre-vingt-dix-neuf virgule cinq pour cent), 24h/24, 7j/7. La disponibilité est calculée en dehors de ses périodes de maintenance programmées.

La disponibilité du Service est mesurée à partir de la surveillance par une société tierce. Un test de disponibilité du Service est réalisé toutes les minutes depuis différentes sources sur internet situés sur des réseaux d'opérateurs Internet différents.

La durée d'indisponibilité (DI) mensuelle est calculée de la façon suivante :

DI (minutes) = Durée d'indisponibilité cumulée du Service en minutes pendant le mois

Le TD global mensuel est calculé de la façon suivante :

TD (%) = [1- (DI / (nb de jours dans le mois * 1440))] x 100

Les statistiques de disponibilité seront communiquées au Client sur demande.

3. PROCESSUS DE MAINTENANCE EN PHASE RUN

3.1. Procédures de Gestion des Incidents

Les demandes de support suivent la procédure mentionnée ci-dessous. Selon le type de demande, les étapes 2 à 5 peuvent être les étapes finales du workflow.

Etape	Acte	Action
1	Client	Créer la demande
2	Niveau 1 - Customer Care	Classer la demande / Recueillir des informations complémentaires
3	Niveau 1 - Customer Care	Qualification des sujets complexes
4	Niveau 2 – Support technique	Analyse technique
5	Niveau 3 - R&D	Action corrective
6	Niveau 1 - Customer Care	Confirmation de la résolution

3.1.1. Matrice RACI pour les Activités de Support :

- **R** : *Responsable*
- **A** : *Approbateur*
- **C** : *Consulté*
- **I** : *Informé*

Activités / Acteurs	Administrateur du Client	Customer Care Cegid niveau 1	Customer Care Cegid niveau 2	Niveau 3 : Produit / Support technique / Production	Customer Care Manager / Customer Success Manager
Déclaration des demandes	R, A	I, C			
Traitement de l'incident	C, I	R, A	C	C	C
Validation de la résolution	R, A	I			
Gestion de crise	C, I	R	C	C	R, A

3.1.2. Contrôle de la Qualité du Service support

Il existe plusieurs mesures de contrôle pour garantir la qualité du service :

- examen hebdomadaire des indicateurs par la direction Customer Care, avec plans d'amélioration et suivi des actions ;
- examen des évaluations à chaud des Clients et plans d'amélioration ;
- examen quotidien des files d'attente de tickets ;

- règles d'alerte préventive en cas d'escalade Client potentielle ou de violation de SLA identifiée dans l'outil de gestion des tickets.

3.2. Procédure de Gestion des Changements

3.2.1. Gestion des versions

Cegid Digitalrecruiters effectue quotidiennement une mise à niveau de la version de la Solution qui implique la distribution de correctifs et de nouvelles fonctionnalités.

Chaque développement est testé et un processus de qualification rigoureux est utilisé pour chaque version sur une plateforme de préproduction avant le déploiement sur la plateforme de production.

Cegid Digitalrecruiters utilise de nombreux tests automatiques qui doivent être passés avec succès avant que la nouvelle version puisse être déployée

3.2.2. Périodes de Maintenance

Cegid Digitalrecruiters s'engage, au titre du Contrat, à assurer la maintenance de la Solution pendant toute la durée du Contrat. Il s'engage à ce titre à effectuer à ses frais toute intervention ou réparation nécessaire pour maintenir la Solution en parfait état de fonctionnement.

Les opérations de maintenance induisant une interruption de services ou une dégradation des performances seront effectuées :

- Sans préavis en cas d'absolue nécessité
- Avec un préavis de 7 jours pour toute intervention susceptible de dépasser 30 (trente) minutes.

3.3. Procédure de Gestion de Crise

L'objectif du processus de gestion de crise est de prévenir et d'atténuer les dommages de la crise en déclenchant un suivi efficace et régulier des actions qu'il n'est pas possible de traiter par des processus standard afin de résoudre rapidement la crise.

La procédure de gestion de crise de Cegid comprend la gestion de tous les types d'incidents, y compris ceux qui ont un impact sur le service, mais aussi les alertes de sécurité. La procédure inclut un processus d'escalade qui peut faire remonter l'incident jusqu'à la direction exécutive de Cegid. La procédure de gestion de crise est organisée autour d'une interface unique créée par l'équipe du Service Client.

Les processus de gestion de crise sont déclenchés dans les circonstances suivantes :

- En cas de force majeure, d'incident bloquant pour lequel une solution de contournement ou un correctif n'a pas été fourni dans un délai raisonnable ou de situations dégradées prolongées sur une durée inacceptable ;
- Incident de blocage généralisé ou situation dégradée ;
- Toutes les alertes de sécurité (connues ou potentielles) qui mettent en danger les données Client ;

3.4. Cessation des Relations Contractuelles

3.4.1. Plan de Réversibilité

Le contrat stipule que les données stockées dans la base de données du Client appartiennent à ce dernier (voir le contrat d'abonnement). En cas de cessation des relations contractuelles, le Client devra donc avoir, avant le dernier jour du Service, récupéré ses données accessibles au travers des fonctionnalités du Service ou demandé

à Cegid la restitution de ses Données, Cegid retransmet au Client toutes les données et informations reçues du Client dans le cadre de l'exécution du présent contrat. Pour permettre au Client d'exploiter les données en question, les données sont retransmises dans un format standard du marché décrit par la procédure de réversibilité.

Cegid Digitalrecruiters s'engage à ne pas conserver de copies des données du Client et à ne pas utiliser les données à quelque fin que ce soit.

3.4.2. Politique de Destruction des Données

En cas de résiliation du contrat ou de changement de plateforme logicielle, Cegid s'engage à supprimer toutes les données Client (y compris la base de données, l'URL et les sauvegardes). Cegid fournira aux Clients une déclaration de destruction des données. Les données sont supprimées 3 mois après la fin du contrat.

4. SITES D'HEBERGEMENT

4.1. Lieux d'Hébergement

Cegid Digitalrecruiters dispose actuellement de plusieurs sur le territoire de l'Union Européenne.

Zone géographique	Pays	Lieu principal	Prestataire
Europe	France	Roubaix (Strasbourg/Gravelines)	OVHCloud

4.2. Sécurité et Confidentialité des Prestataires d'Hébergement

Nous évaluons et sélectionnons nos centres d'hébergement selon des critères stricts de sécurité, de confidentialité, de qualité et de disponibilité.

Le fournisseur cloud et Cegid Digitalrecruiters sont liés par un contrat qui comprend une clause de confidentialité.

La structure juridique de Cegid Digitalrecruiters est basée en France et les centres de données pour les Clients sont basés dans l'Union européenne (y compris la France). Cegid Digitalrecruiters garantit que les données seront toujours situées en Europe pour tous les Clients européens. Cette garantie s'applique également aux sauvegardes.

Nos centres d'hébergement ont en commun les caractéristiques suivantes :

- centres de données conçus avec des niveaux élevés de redondance pour des solutions à très haute disponibilité (tiers III ou équivalent) ;
- système de communication haut débit reposant sur un réseau de fibre optique longue distance entièrement redondant ;
- normes les plus élevées en matière de sécurité active ;
- souci permanent de l'efficacité énergétique et volonté de limiter tout impact environnemental.

Les centres de données utilisés par Cegid possèdent de solides certifications : https://www.ovhcloud.com/fr/enterprise/certification-conformity/

5. ARCHITECTURE TECHNIQUE

L'application Cegid Digitalrecruiters est basée sur une architecture à trois (3) niveaux :

- les postes de travail des Utilisateurs utilisent un navigateur Web et doivent avoir un accès à Internet ;
- les serveurs d'applications répondent aux demandes HTTPS ;
- les serveurs de données ne sont accessibles que depuis les serveurs d'applications. Ils hébergent les moteurs de recherche de la base de données, ainsi que les données Client.

Les principes sous-jacents de l'architecture technique de Cegid Digitalrecruiters permettent :

- la séparation logique des Clients à des fins de sécurité, de confidentialité et de disponibilité ;
- un haut niveau de personnalisation de l'environnement de chaque Client sans impact sur les autres Clients, tout en maintenant l'uniformité du progiciel ;
- l'hébergement dans des centres de données qui répondent aux exigences de Cegid Digitalrecruiters.

5.1. Architecture d'Application

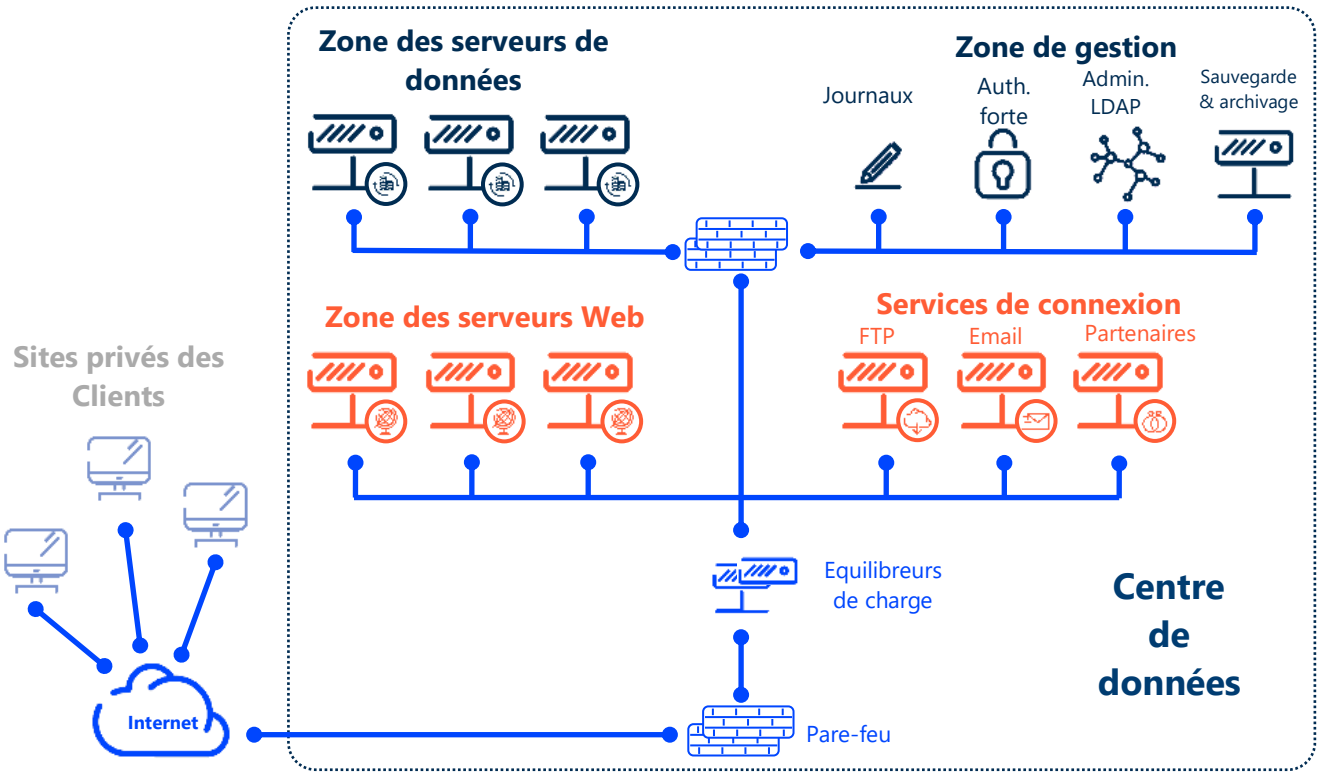
La solution Cegid Digitalrecruiters est composée de plusieurs unités logiques qui sont toutes intégrées dans une seule application :

- Le Back Office (ATS). Cette partie est principalement utilisée par les équipes RH et les managers. Le Back Office est utilisé pour tous les processus de recrutement.
- Les Front Offices (Sites Carrières). Les Front Offices permettent aux candidats et aux employés (sites de mobilité interne) de consulter les offres d'emploi, de postuler et de soumettre leurs CV, et de s'inscrire à des listes de diffusion. Il est possible d'exécuter plusieurs Front Offices qui correspondent à plusieurs portails Internet ou Intranet, chacun ayant des fonctionnalités et des chartes graphiques différentes.
- Toutes les informations peuvent être constituées au sein d'une base de données commune.

Le Front Office est un bloc indépendant car il est exposé à l'Internet public, et fait généralement partie d'un site Web d'entreprise. Il peut donc être reconfiguré et personnalisé pour le Client. Il est toutefois relié à un Back Office afin de gérer les candidats, les offres d'emploi et les candidatures.

5.2. Architecture Serveur et Réseau

Voici un schéma de l'architecture exécutée pour l'hébergement des applications :



La technologie de virtualisation utilisée est VMware.

Tous les serveurs Web sont dotés d'une technologie avancée d'équilibrage des charges. Tous les serveurs de base de données sont configurés avec une réplication synchrone.

La zone de stockage et d'archivage est physiquement séparée de la zone de production. La zone d'administration n'est accessible qu'aux administrateurs Cegid Digitalrecruiters autorisés, après une connexion via un serveur de rebond et une séquence d'authentification forte. Chaque administrateur utilise un compte nommé.

Seuls les serveurs Web ont accès aux serveurs de données, qui sont donc inaccessibles depuis Internet.

5.3. Infrastructure Technique de Logiciel

5.3.1. Composants d'Infrastructure

La solution Cegid Digitalrecruiters a été développée sur l'architecture technique suivante :

- Système d'exploitation Linux
- Base de données MySQL Server
- Serveur d'applications Nginx
- Langage de programmation PHP.

Voici un résumé des principaux composants de l'infrastructure pour la version actuelle du produit :

Composant	Produit	Version
Système d'exploitation serveur	Linux Debian	10 & 11
Serveur Internet	Nginx	
Moteur de base de données	MySQL	5.7
Moteur de base de données non relationnelle	ElasticSearch	7.4
Moteur de cache	Redis	5.7.0.7
Moteur de queuing	RabbitMQ	3.11.5

5.3.2. Bases de Données d'Application

Une application Cegid Digitalrecruiters repose sur un cluster de base de données multi-tenants qui contient des données techniques (configuration, opérations, ...) et des données Clients (vivier de candidats, offres d'emploi, candidatures, ...).

Les données des Clients sont séparées logiquement et font l'objet d'un chiffrement au repos.

5.4. Gestion Multi-Clients

L'application Cegid Digitalrecruiters est disponible sous forme de sites Web. Pour le partie Front Office chaque Client possède son propre sous-domaine qui est servi par une instance unique du serveur Web. Le produit possède une architecture logicielle multi-tenant et tous les sous-domaines pointent vers la dernière version de l'application.

5.5. Environnement de Test

Selon les conditions contractuelles, les Clients peuvent souscrire à un environnement de test.

L'environnement de test est installé et géré comme un environnement séparé de l'environnement de production. Il est géré comme s'il s'agissait de l'environnement d'un Client différent.

Les environnements de test sont utilisés pour tester une action, un paramétrage ou à des fins de formations. Les données dans l'environnement de test peuvent être une copie des données de production à un moment donné et sont donc plus anciennes.

Les environnements de test ne sont pas aussi disponibles que les zones de production. En outre, Cegid Digitalrecruiters se réserve le droit d'interrompre momentanément ces environnements pour effectuer diverses tâches (installations pendant les heures de travail, par exemple).

5.6. Application Mobile

L'application mobile Cegid DigitalRecuiters est disponible sur deux plateformes mobiles : Android et iOS. L'application peut être téléchargée dans leurs bibliothèques d'applications respectives.

L'authentification unique est supportée à condition que le client ait mis en place un fournisseur d'identité.

L'application mobile Cegid Digitalrecruiters ne fournit qu'une couche de présentation. Cela signifie qu'aucune donnée n'est stockée sur l'appareil mobile. Les données personnelles sont stockées dans les centres de données de Cegid Digitalrecruiters et sont accessibles en temps réel via des APIs.

6. GESTION DES ACCES

6.1. Sécurité des Accès aux Applications

6.1.1. Front Office Candidat

Par définition, les applications du Front Office Candidat sont exposées et accessibles via Internet.

6.1.2. Back Office et Espaces Employé/Manager

L'application BackOffice est exposée et librement accessible via Internet ;

6.2. Authentification

La politique de contrôle d'accès à la plateforme peut être :

- Gérée via l'application Digitalrecruiters : saisie d'un login et d'un mot de passe.
- Déléguée à nos clients dans le cas d'activation d'un mécanisme d'authentification unique (SSO), auquel cas, la politique du client s'applique.

6.2.1. Responsabilités des Clients

Dans le cas où l'authentification est déléguée, les Clients sont responsables de leur propre politique en matière de mots de passe.

6.2.2. Authentification pour le Front Office Candidat

L'accès au Front Offices n'est pas soumis à une authentification.

6.2.3. Authentification dans Back Office

Plusieurs mécanismes d'authentification sont disponibles pour les Utilisateurs travaillant avec l'entreprise :

- via le login et le mot de passe Cegid Digitalrecruiters ;
- par l'authentification unique (SSO) mise en place par le Client.

La session est entièrement gérée sur le serveur. Seul un cookie de session est stocké sur le poste de travail de l'Utilisateur et, dans certains cas, un état de vue est contenu dans la page.

6.2.4. Gestion des Mots de Passe

Cegid Digitalrecruiters propose les politiques de gestion des mots de passe suivantes :

- changement de mot de passe lors de la première connexion ;
- longueur minimale du mot de passe de 8 caractères ;
- nombre minimum de caractères non alphanumériques, numériques, minuscules et majuscules dans le mot de passe ;
- réinitialisation du mot de passe via un lien d'activation envoyé par email ;
- validation obligatoire de l'adresse email avant l'activation d'un compte ;

Les mots de passe sont sécurisés dans la base de données de manière non réversible grâce à l'algorithme Bcrypt.

Mots de passe perdus/oubliés. Lorsque les Utilisateurs oublient leur mot de passe et n'utilisent pas l'authentification unique (SSO), ils doivent procéder comme suit :

- utiliser un navigateur Internet pour accéder à leur page de connexion Cegid Digitalrecruiters ;
- cliquer sur le champ « Mot de passe oublié », saisir son adresse email puis cliquer sur « VALIDER » ;
- un lien de réactivation sera envoyé par email à l'Utilisateur. L'Utilisateur devra saisir un nouveau mot de passe avant de se reconnecter à l'application.

6.2.5. Authentification Unique

Si le Client a mis en place un fournisseur d'identité, il est alors possible d'authentifier les Utilisateurs via l'authentification unique basée sur les protocoles SAML 2.0.

6.2.6. Durée de la Session

Une session dans le portail Back Office est interrompue après huit heures d'inactivité. La durée de la session est de vingt heures.

6.3. Politique en Matière de Cookies

Lors de la navigation sur nos applications, des cookies sont stockés sur le navigateur de l'Utilisateur. Les cookies ont pour but de collecter des informations de navigation, d'identifier les Utilisateurs et de leur permettre d'accéder à leurs comptes.

En ce qui concerne les données relatives aux cookies, Cegid Digitalrecruiters s'engage à respecter la réglementation locale de chaque pays, à protéger la confidentialité des données et à respecter les obligations territoriales en matière de lieu de stockage des données.

Les traitements relatifs relatifs aux cookies sont décrits sur cette page :

https://www.Digitalrecruiters.com/politique-de-confidentialite

6.4. Rôles, Droits et Habilitations

Cegid Digitalrecruiters dispose d'une interface dédiée à l'administration des rôles, droits et habilitations.

6.4.1. Rôles et Droits

Les rôles sont utilisés pour définir des profils standard avec certains niveaux d'accès aux fonctionnalités de Cegid Digitalrecruiters. Tout d'abord, les rôles sont définis, puis ils sont attribués aux Utilisateurs de Cegid Digitalrecruiters. Les droits attribués aux rôles sont configurables dans la solution. Les rôles peuvent être entièrement reconfigurés à l'aide du module de gestion des droits.

6.4.2. Habilitations

Les listes d'habilitation des Utilisateurs permettent de définir qui a le droit d'accéder aux informations de tel ou tel ressource.

7. INTERFACES

Dans Cegid Digitalrecruiters, il est possible d'importer et d'exporter des données sous forme de fichiers au format CSV ou en utilisant des Web Services.

Ce chapitre décrit les principes qui sous-tendent les échanges de fichiers et Web Services, ainsi que les aspects de sécurité liés à ces échanges. Les spécifications des interfaces sont fournies au début du projet de déploiement.

7.1. Importation/Exportation de Fichiers

7.1.1. Import

La solution Cegid Digitalrecruiters permet l'importation à l'aide de fichiers CSV sur les fonctionnalités suivantes :

- Import des candidatures ;
- Import de l'arborescence ;
- Import des utilisateurs ;

La mise en place de ces imports fait l'objet d'une description complète dans des documents dédiés et est à organiser avec les équipes Cegid Digitalrecruiters durant le déploiement de la solution.

7.1.2. Export

La solution Cegid Digitalrecruiters permet l'exportation dans des fichiers CSV des données suivantes :

- Arborescence ;
- Statistiques.

7.2. Interface FTP Sécurisée

En cas de nécessité, la mise en place d'une plateforme d'échange de fichier et est à organiser avec les équipes Cegid Digitalrecruiters durant le déploiement de la solution.

7.3. Interfaces de Programmation d'Applications (API)

Cegid fournit un certain nombre de Web Services permettant à des applications tierces d'utiliser les services Cegid Digitalrecruiters. Ces Web Services couvrent les domaines fonctionnels suivants :

- Export des candidatures recrutées ;
- Agrégation d'annonces des sites carrières ;
- Export des annonces ;
- Nombre d'annonces par service ;
- Modification des annonces ;
- Import de candidatures ;
- Export de candidatures.

La mise en place de ces API fait l'objet d'une description complète dans des documents dédiés et est à organiser avec les équipes Cegid Digitalrecruiters durant le déploiement de la solution.

7.4. Interface de messagerie

L'application Cegid Digitalrecruiters envoie des emails en utilisant le protocole SMTP classique. Les emails peuvent être envoyés au format HTML.

8. OPERATIONS

8.1. Procédures d'Exploitation

Ce chapitre décrit les procédures d'exploitation utilisées le plus souvent au cours du service.

Purge des journaux du système. Les journaux du système sont conservés pendant quatre-vingt-dix (90) jours.

Purge du journal d'application. Le journal d'application contient les données de suivi des actions de l'Utilisateur. Ce journal conserve un (1) an de données, les données plus anciennes sont purgées.

8.2. Management de la Donnée

8.2.1. Sauvegarde des Données

Ce chapitre s'applique aux données de production.

Organisation des Sauvegardes

Les sauvegardes des différents types de données sont effectuées sur la base d'une stratégie qui implique la meilleure sécurité et intégrité des données, ainsi que le temps de restauration. Il s'agit de sauvegardes en ligne sans aucune interruption de service de la base de données.

Données	Action	Fréquence	Conservation
Machines virtuelles	Sauvegarde complète	Toutes les 2h	14 jours
Base de données	Sauvegarde complète	Toutes les 24h	30 jours
Base de données	Sauvegarde partielle	Toutes les 2h	24 heures
NAS	Réplication complète	1 fois par jour	-
Logs	Sauvegarde complète	1 fois par jour	3 mois

Les supports et emplacements de sauvegarde dépendent du fournisseur cloud :

	Stockage de sauvegarde	Réplication des données
OVHcloud	Object Storage	Les données chiffrées sont répliquées nativement par le service Object Storage sur différentes zones géographiques.

Seul un nombre très limité de personnes a accès aux sauvegardes des bases de données. Ces personnes, comme tout le personnel de Cegid, sont liées par une clause de confidentialité. De même, notre fournisseur cloud dispose d'un nombre limité de personnes autorisées à accéder aux sauvegardes.

8.2.2. Chiffrement des Données

Chiffrement des Données en Transit

Pour assurer la sécurité des données en transit, Cegid chiffre le flux des applications avec le protocole HTTPS pour tous les domaines et exige le protocole Transport Layer Security (TLS) 1.2 ou supérieur.

Chiffrement des Données au Repos
Les mots de passe sont sécurisés dans la base de données de manière non réversible grâce à l'algorithme Bcrypt.

Cegid fournit un chiffrement des volumes en AES XTS.

8.3. Administration et Supervision

La plateforme est supervisée 24 heures sur 24, 7 jours sur 7. Le suivi des performances et la supervision des applications ont été mis en place et déclenchent des alertes lorsque des problèmes sont détectés.

Un processus de traitement et d'escalade a été défini et est suivi par les équipes opérationnelles.

Les outils utilisés pour la supervision des infrastructures sont Splunk Observability et Centreon. Nos fournisseurs d'hébergement disposent également de leur propre système de surveillance.

Les procédures d'exploitation comprennent les tâches suivantes (liste non exhaustive) :

- administration ;
- maintenance des systèmes d'exploitation (espace disque, journaux, etc.) ;
- maintenance des bases de données ;
- tests, qualification et déploiement des mises à jour de sécurité ;
- maintenance des applications (journaux et analyse des performances) ;

Supervision :

- surveillance de la disponibilité des applications ;
- surveillance du temps de réponse ;
- surveillance de la charge de la plateforme (mémoire, processeurs, disques) ;
- surveillance de la bande passante du réseau ;
- surveillance des tâches batch des applications et systèmes ;
- surveillance du matériel.

Les fournisseurs d'hébergement sont responsables des tâches associées aux éléments suivants :

- équipement physique (matériel de serveur, équipement de réseau, etc.) ;
- hyperviseurs ;
- réseau ;
- mises à jour logicielles pour les systèmes d'exploitation, bases de données et antivirus ;
- suivi des éléments ci-dessus ;
- vérification et qualification des sauvegardes ;
- surveillance et mise à jour des systèmes antivirus ;
- maintenance des équipements de réseau.

8.4. Plan de Continuité des Activités

Une infrastructure de production haute disponibilité est mise en place, celle-ci repose sur le découpage de l'ensemble en services, chaque service étant assuré par un cluster de serveurs indépendants, garantissant la

résilience de l'infrastructure. Ainsi en cas de dysfonctionnement d'une machine (ou de plusieurs machines simultanément), les autres serveurs du cluster absorbent temporairement la charge supplémentaire, garantissant la continuité de service.

Cette organisation permet également la scalabilité de l'infrastructure, en augmentant simplement sa capacité par le déploiement de nouvelles machines à la volée. Pour une efficacité maximum, les outils Ansible, Chef et Terraform sont utilisés afin d'automatiser le déploiement et la configuration de machines supplémentaires.

9. REGLEMENTATIONS ET REFERENTIELS

9.1. Règlement Général sur la Protection des Données (RGPD)

Vous trouverez ci-dessous une description des mesures en application du RGPD afin d'aider les Clients dans leur conformité RGPD avec Cegid Digitalrecruiters.

Important : tous les éléments de sécurité des données sont décrits dans le Plan d'Assurance Sécurité ou dans d'autre chapitre du présent document; pour cette raison, ils ne sont pas mentionnés ici. Cependant, ils concernent tous le RGPD dans le sens où la sécurité des données est une exigence clé pour tous les sous-traitants (les "processeurs").

Pour la mise en œuvre des exigences du RGPD dans sa solution, Cegid Digitalrecruiters, en tant que sous-traitant (Data processor), distingue deux personas différents : le candidat et le salarié. Certaines des exigences du RGPD ne dépendent pas des personas, et certaines d'entre elles génèrent des comportements de produits différents selon que l'on s'adresse à un candidat ou à un employé.

9.1.1. Exigences du RGPD Applicables à tous les Personas

Le respect de la vie privée dès la conception

Le processus actuel de développement agile/logiciel couvre la formation du personnel, les examens formels du code et les outils qui détectent la nécessité d'appliquer les meilleures pratiques.

Les principes relatifs au traitement des données personnelles tels que définis dans l'article 5 du GDPR sont pris en compte par la conception dans le développement du produit.

La confidentialité par défaut

Par défaut, le niveau de protection des données est toujours fixé au niveau le plus restrictif.

Délégué à la protection des données

Cegid a nommé un DPO étant donné la nature de leurs activités.

Enregistrement des activités de traitement

Cegid maintient un enregistrement des activités de traitement en qualité de sous-traitant

DPA avec les Sous-traitants ultérieurs

Cegid délègue une partie de son activité à des sous-traitants. Des DPA sont signés entre eux et Cegid qui contiennent des clauses en conformité avec le RGPD.

Données sensibles

Cegid Digitalrecruiters ne collecte pas de données sensibles, telles que celles mentionnées à l'article 9 du RGPD. Cegid Digitalrecruiters offrant une certaine flexibilité sur les compléments disponibles pour le modèle de données, Cegid ne recommande pas à ses clients de définir des champs supplémentaires correspondant à des " données sensibles ", telles que définies à l'article 9 du RGPD.

Notification des violations de données

Cegid a mis en place une procédure de notification de violation de données. Cette procédure est définie, maintenue et suivie dans le cadre du système de gestion de la sécurité de l'information et du RGPD.

En cas de violation de données personnelles, Cegid s'engage à notifier le client (le responsable du traitement) dans les meilleurs délais comme le prévoit le RGPD, afin que le client puisse ensuite signaler la violation de données personnelles à l'autorité de contrôle compétente et à la personne concernée dans les 72 heures, si cette notification est obligatoire. Il appartient au client de juger si cette notification à l'autorité de contrôle et/ou à la personne concernée est nécessaire.

Processus de décision automatisé

L'application Cegid Digitalrecruiters ne comporte aucune fonction de prise de décision individuelle automatisée ou de profilage automatisé. Toutes les décisions sont laissées aux utilisateurs humains, qui peuvent utiliser les tableaux de bord, les KPI, les recommandations et les analyses pour prendre une décision éclairée.

Anonymisation des données

Cegid Digitalrecruiters propose une fonction d'anonymisation "base de données complète". Elle est utilisée lorsqu'une base de données de production doit être utilisée pour les tests, le débogage ou la formation.

Informations à fournir lorsque des données personnelles sont collectées auprès de la personne concernée

Il appartient au client de fournir directement ces informations à ses candidats et employés. Notre solution offre la possibilité à notre client de fournir ces informations, via une configuration de celle-ci.

9.1.2. Réponse aux Exigences du RGPD sur les Candidats

Les candidats n'ont pas de lien de subordination avec l'employeur potentiel, qui est responsable du traitement des données. C'est pourquoi nous avons clairement exposé toutes les méthodes possibles de traitement des données utilisées par le produit.

Droit d'accès, droit de rectification

Les candidats peuvent envoyer un e-mail à l'administrateur client (ou DPO du responsable de traitement) pour demander la suppression ou la rectification de leurs données personnelles. L'administrateur (ou DPO) client peut contacter les équipes du service client de Cegid pour obtenir de l'aide. Un recruteur peut également supprimer ou rectifier les données personnelles d'un candidat, si nécessaire.

Droit à l'oubli

Les droits d'effacement peuvent être automatisés par entité :

- Cela permet aux clients de gérer les périodes de conservation des données par pays.
- À la fin de la période de conservation, les candidats recevront un courriel leur demandant s'ils souhaitent donner leur consentement au renouvellement de la rétention de leurs données personnelles.
- Si un candidat soumet des demandes d'emploi dans plusieurs pays avec des périodes de conservation des données variables, la période de rétention appliquée sera celle de l'entité liée à la dernière action de candidature. Si le candidat donne son consentement au renouvellement de la rétention des données personnelles, ses données personnelles seront stockées dans le back-office. Si le candidat ne donne pas son consentement, ses données personnelles seront supprimées. Si le candidat ne répond pas, ses données personnelles seront supprimées à la fin de la période de conservation des données.

Les données personnelles sont supprimées de manière asynchrone lors des procédures de nuit programmées.

Bases légales

Le responsable de traitement a l'obligation de déterminer avant la mise en production de la solution Cegid Digitalrecruiters une base légale la plus appropriée au regard de son contexte (art. 6.1 du RGPD).

A titre d'information, afin d'aider à la détermination des bases légales, la CNIL a adopté un référentiel « *relatif aux traitements de données personnelles mise en œuvre aux fins de gestion du personnel* » le 21 novembre 2019.

Dans ce dernier, la CNIL propose 2 bases légales relatives au recrutement :

-« ***Traitement des candidatures (CV et lettre de motivation) et gestion des entreprises*** *: Mesures précontractuelles*

-***Constitution d'une CV-thèque*** *: Intérêt légitime* »

Tout transfert de données intragroupe devra aussi être justifié avec une base légale et porté à la connaissance des candidats.

9.1.3. Réponse aux Exigences du RGPD sur les Employés

Droit d'accès, droit de rectification

Le produit fournit les fonctionnalités nécessaires pour accéder aux données des employés et les modifier. L'accès à ces fonctionnalités est géré par des rôles et des droits, qui peuvent être attribués directement par les administrateurs du client.

Droit à l'effacement

Pour diverses raisons, les entreprises collectent et traitent les données personnelles de leurs employés. Toute demande de suppression de données personnelles émise par un employé doit être approuvée par l'employeur (le responsable du traitement).

C'est pourquoi notre produit offre une fonction de suppression dans l'interface utilisateur de Cegid Digitalrecruiters. Cette fonctionnalité est soumise à un droit spécifique, qui peut être attribué par les administrateurs du client à leurs utilisateurs concernés. Actuellement, le produit effectue une suppression physique et irréversible de la base de données.

Bases légales

Le responsable de traitement a l'obligation de déterminer avant la mise en production de la solution Cegid Digitalrecruiters une base légale la plus appropriée au regard de son contexte (art. 6.1 du RGPD).

Dans le même référentiel de la CNIL cité ci-dessus (« *Référentiel relatif aux traitements de données personnelles mise en œuvre aux fins de gestion du personnel* » du 21 novembre 2019), la CNIL indique concernant le consentement que : « *Les employés ne sont que très rarement en mesure de donner, de refuser ou de révoquer librement leur consentement, étant donné la dépendance qui découle de la relation employeur/employé. Ils ne peuvent donner leur libre consentement que dans le cas où l'acceptation ou le rejet d'une proposition n'entraine aucune conséquence sur leur situation* ».

Ainsi, la CNIL propose d'autres bases légales suivant l'activité sur les employés. Un tableau est disponible dans ce référentiel afin d'aider le responsable de traitement à les déterminer.