cegid

Livret de Service

Cegid Wittyfit

30/11/2023

www.cegid.com

SOMMAIRE

HISTORIQUE DES MODIFICATIONS ET DES VALIDATIONS

Nature des modifications	Version	Date
Création du document	01	20/03/2023
Mise à jour de format	01.1	30/11/2023

Auditeur(s)

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

Approbateur(s)

Date	Nom, fonction
01/04/2023	Laura Martineau, Directrice Customer Success Cegid Wittyfit
01/04/2023	Thibault Perret, Responsable R&D Cegid Wittyfit

Liste de distribution

Personne ou groupe
Client Cegid Wittyfit
Interne Cegid Wittyfit

1. INTRODUCTION

1.1. Objet du Livret de Services

Le présent Livret Service qui fait partie intégrante du Contrat décrit les dispositions particulières applicables aux Services Cegid Wittyfit qui prévalent sur les dispositions générales du Contrat en cas de contradiction et/ou complètent les dispositions générales du Contrat.

Les dispositions applicables en matière de protection des Données Personnelles sont celles figurant à l'annexe Politique de protection des Données Personnelles du Contrat.

Concernant la sécurité, le Service Nominal fait l'objet d'un Plan d'Assurance Sécurité (PAS).

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

- qualité du support fournie par Cegid ;
- 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 Wittyfit, tant pour l'infrastructure Client partagée que pour l'infrastructure spécifique au Client.

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/DE L'ACCOMPAGNEMENT

2.1. Localisation des Équipes et accessibilité au Support

Les équipes de support Customer Care de Cegid Wittyfit sont basées en France. Les demandes de support peuvent être rédigés en français.

Les tickets de support doivent être émis via l'outil de ticketing présent au sein de la plateforme Wittyfit. Au clic sur le pictogramme **« ? »** l'utilisateur sera redirigé vers le centre d'aide Jira, un outil de ticketing disponible via Internet pour tous les Clients ayant un contrat Wittyfit.

Il est aussi possible pour chaque utilisateur de la plateforme Wittyfit d'envoyer directement un email au support via l'adresse suivante : wittyfitsupport@cegid.com.

2.2. Contrat d'Accompagnement / Support

Cegid propose une offre de support standard qui se nomme « Open » (incluse dans la licence) pour Wittyfit.

Elle permet de :

- créer des demandes de support via la plateforme Wittyfit ;
- accéder à la documentation produit via Jira ;
- participer à des ateliers webinar de montés en compétences sur l'outil Wittyfit
- participer au club utilisateur Wittyfit

De plus, cette offre OPEN donne accès à :

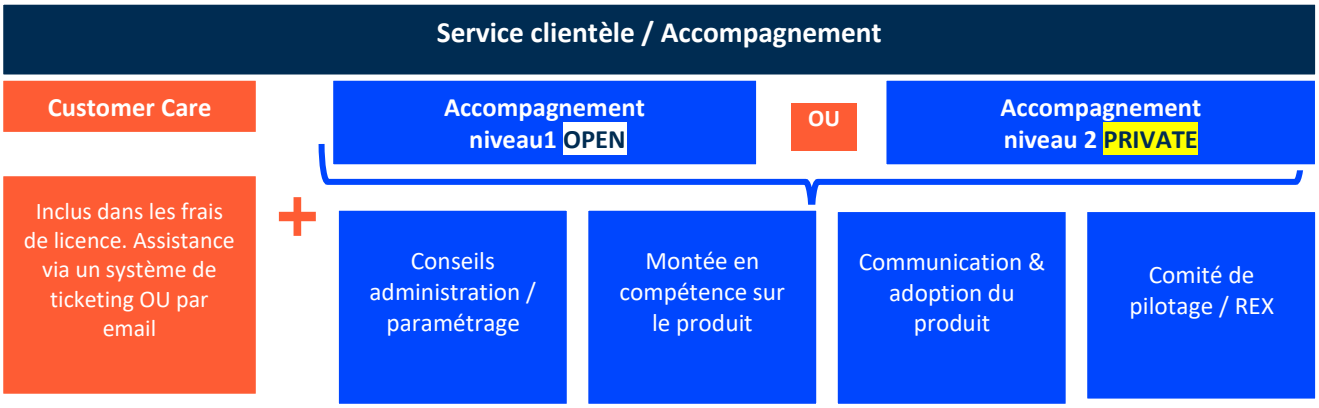
- consultant Cegid Wittyfit dédié ;
- démonstrations contextualisées des nouvelles fonctionnalités ;
- comité de pilotage / retour d'expérience ;
- indicateurs de suivi de l'engagement de service.

Cegid propose un deuxième niveau d'accompagnement l'offre « Premium » (disponible en option). Dans cette offre l'accompagnement est plus soutenu.

Une demande pour ce service peut être faite en contactant votre représentant commercial.

Ce deuxième niveau d'accompagnement permet d'accéder à niveau d'accompagnement plus important *CF le tableau ci-dessous :*

Résumé de nos deux offres d'accompagnement / support en phase Run :



Détails et différences entre l'accompagnement « Open » & « Premium » :

	Offre niveau OPEN	Offre niveau PRIVATE
Interlocuteur CSM dédié *(Un CSM pour vous vous guider dans les grandes étapes : Kickoff, Call RH, organiser des sessions de formation et réunion de retour expérience post campagne)*	X	X
Interlocuteur CSM dédié *pour un accompagnement spécifique : adaptation questionnaire, création de questions, sujet « manager » spécifique*		X
Webinar de démo* + Q&A *(CHSCT; CSE; Managers;...)*		X 2 interventions*
Accompagnement dans le plan de communication *(Call avec l'équipe de com interne du client => afin d'évoquer les différentes étapes de communication : adapter les messages & les supports)*		X
Formation à l'administration RH *(autonomie pour ajouter ou supprimer un collaborateur, modifier une affectation, ajouter un droit manager...)*	X	X
Formation à l'outil Wittyfit* *(connaître les fonctionnalités, savoir interpréter, savoir créer des plans d'action, comment intégrer wittyfit dans une pratique managériale...)*	X Pack de **2 interventions** par an **	X Pack de **5 interventions** par an **

* 2 interventions si c'est une entreprise avec plus de 1000 collaborateurs . Si inférieur à 1000 alors nous proposons qu'une seule intervention.

** **Pack de session de formation à adapter :**

=> PRIVATE **: pack de 5 interventions si + de 1000 collaborateurs sinon passer à 3 interventions**

2.3. Accès aux Ressources Applicatives

Un accès à une banque de ressources personnalisées est communiqué par votre interlocuteur CSM dédié. Il s'agit d'un espace regroupant toutes les informations nécessaires pour vous aider à déployer Cegid Wittyfit au sein de votre organisation : des guides d'utilisation, des vidéos tutoriels et autres contenus informatifs.

Un deuxième accès peut être communiqué aux clients afin qu'ils puissent le partager en interne à d'autres utilisateurs.

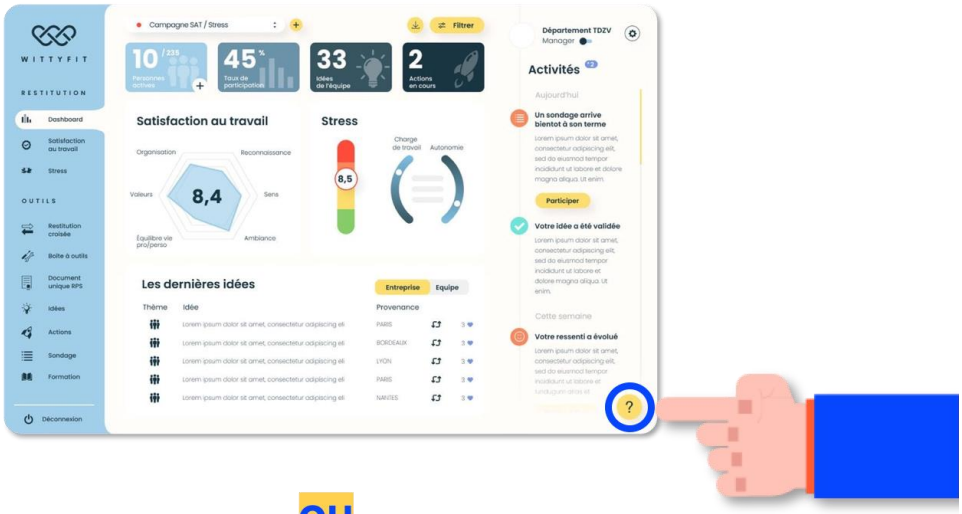
2.4. Section Support

Les tickets de support doivent être émis via l'outil de ticketing présent au sein de la plateforme Wittyfit. Un outil de support disponible pour tous les utilisateurs de la plateforme Wittyfit : accès type collaborateur ; accès type manager et accès type superviseur. Pour créer un nouveau ticket, les formulaires sont accessibles :

- au bas de chaque page de la plateforme Cegid Wittyfit ;
- sur les guides de connexion à la plateforme Cegid Wittyfit ;

- via le mail : wittyfitsupport@cegid.com

Accéder au support directement sur la plateforme Wittyfit :



OU

Par email à l'adresse suivante : wittyfitsupport@cegid.com

Le support de la solution Wittyfit est accessible 24 h/24 et 7 j/7 ; les demandes sont traitées par une équipe fonctionnelle, du lundi au vendredi de 9h00 à 18 h00 CET / 9 h 00 à 17 h 00 EST.

Cet outil est compatible avec **Google Chrome** ou **Firefox**. Le navigateur tel que **Microsoft Edge** ne prend pas en charge toutes les fonctionnalités des pages de la plateforme Wittyfit et des problèmes de lenteur de chargement ou de pages invalides peuvent survenir.

Lorsqu'ils soumettent des demandes, les utilisateurs doivent préciser les informations suivantes :

- le type et la gravité de la demande,
- le titre de la demande principale
- les actions entreprises ayant mené à la génération de l'anomalie,
- une brève description du problème,
- en option : une capture d'écran OU une pièce jointe.

A la clôture du ticket, une évaluation à chaud est envoyée au Client afin d'obtenir son avis et d'améliorer la qualité de notre service.

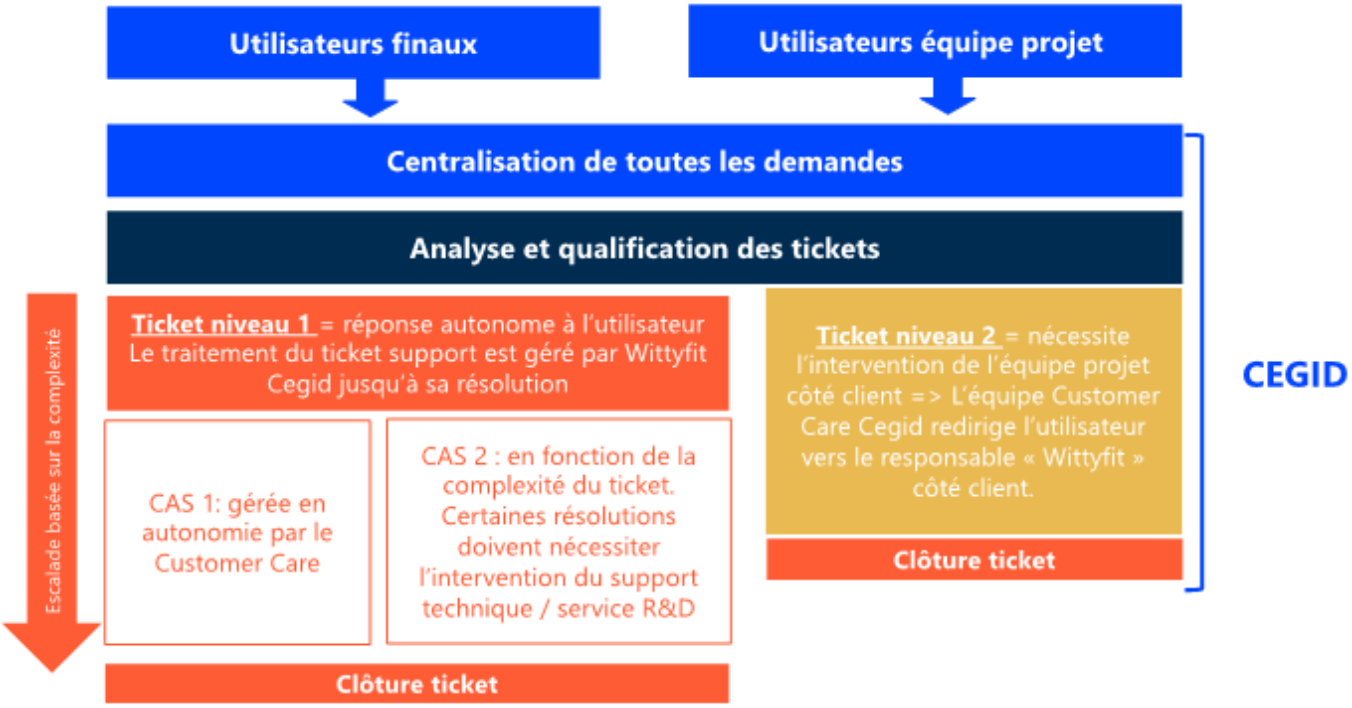
2.5. Workflow des Tickets entre le Client et Cegid

2.5.1. Liste des Statuts

Le tableau ci-dessous explique les différents statuts JIRA (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*
En attente de réponse du support	Le ticket est en cours de traitement par Cegid Ce statut est automatiquement mis à jour par Jira dès qu'un responsable est attribué ou que le Client / utilisateur a ajouté un commentaire.	Cegid
En attente réponse client / utilisateur	Le ticket est en cours de traitement par le Client Ce statut est mis à jour par Cegid lorsqu'une réponse ou une information complémentaire est requise de la part du Client / Utilisateur. Un email est envoyé par Cegid au client / utilisateurs après dix (10) jours ouvrés et (2) rappels en l'absence de réponse du Client / Utilisateur. Le ticket sera automatiquement clôturé après cinq (5) jours ouvrés après envoie de l'email.	Client
En cours de traitement	Le ticket est en cours de traitement par Cegid. Le ticket est en cours d'analyse et/ou de traitement par le support technique ou le service R&D.	Cegid
En attente de validation	Le ticket est en cours de traitement par le Client	Client
Clôturé	Le ticket est clôturé : • lors de la validation par le Client (mise à jour automatique) ; • sur demande de clôture manuelle par le Client à Cegid ; Clôture immédiate	N/A

2.5.2. Workflow des tickets entre le Client et Cegid Wittyfit



2.6. Définition Contractuelle des Anomalies et Politique de SLA

2.6.1. Définitions

Une anomalie est une défaillance, un incident, un dysfonctionnement ou un comportement anormal, qui diffère du comportement attendu tel que documenté par la solution. L'indisponibilité totale ou partielle de l'application, ou la dégradation des performances, qui perturbe ou interrompt l'utilisation de la solution est également considérée comme une anomalie.

Les anomalies devant être qualifiées par Cegid sont classifiées en trois catégories :

Anomalie bloquante :

- 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 Wittyfit

Temps de résolution des anomalies

Les accords de niveau de service (SLA) dépendent de la gravité de l'anomalie, telle que définie par le Client :

	SLA en heures ouvrables	SLA en jours ouvrables
Bloquante	Quinze (15) heures	Un jour et demi
Majeure	Cinquante (50) heures	Cinq (5) jours
Mineure	Cent (100) heures	Dix (10) jours

Les heures de travail de l'équipe du service Clientèle de Cegid Wittyfit sont du lundi au vendredi de 9 h 00 à 18 h 00 CET.

Les accords de niveau de service (SLA) commencent dès que les incidents sont soumis via ticket à la plateforme de support helpdesk pendant les heures d'ouverture ou au début du jour suivant. La période de support prend fin lorsque Cegid confirme une solution définitive ou une solution de contournement.

Le temps pris pour traiter le ticket de « En attente de réponse client » est déduit du temps de traitement total.

Période SLA = (Date d'acceptation de la solution ou de la solution de contournement - Date de création) - Temps pendant lequel le ticket était «En attente de réponse client».

Le prix du SLA est inclus dans le prix de l'abonnement à la licence.

2.6.3. Disponibilité du SaaS

Cegid s'engage à mesurer ses normes de service à l'aide de l'indicateur suivant :

Définition :	Mesure la disponibilité globale du service en utilisant le temps d'arrêt total cumulé sur six mois (7 j/7 - 24 h/24)
Objectif de l'indicateur :	Disponibilité de 99,5 % (accord contractuel)

Calcul de la disponibilité (%)

[* Disponibilité maximale sur 6 mois / (Accessibilité maximale sur 6 mois - Temps d'inaccessibilité (minutes))] x 100

* Nombre total de minutes de disponibilité sur 6 mois = 60 minutes x 24 heures x 30 jours x 6 mois = 259 200 minutes

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 – R&D	Analyse fonctionnelle & technique
5	Niveau 2 - 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	Niveau 2 : 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
Validation de la résolution	R, A	I		
Gestion de crise	C, I	R	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 en continue des indicateurs par l'équipe Customer Care, avec plans d'amélioration et suivi des actions ;

- Examen quotidien par l'équipe Customer Care 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.
- Examen des évaluations à chaud des Clients et plans d'amélioration ;

3.2. Procédure de Gestion des Changements

Chaque sprint de 2 semaines, Cegid effectue une mise à niveau de la version de Cegid Wittyfit qui implique la distribution de correctifs et de nouvelles fonctionnalités.

Chaque développement est testé par l'ingénieur responsable avant d'être compilé dans une version. Un processus de qualification rigoureux est utilisé pour chaque version avant le déploiement. Cegid utilise série de tests automatiques qui doivent être passés avec succès avant que la nouvelle version puisse être présentée au comité de déploiement.

3.2.1. Gestion de Versions

De nouvelles versions de l'application Cegid Wittyfit sont publiées chaque sprint de 2 semaines.

Cegid publie la documentation correspondant aux nouvelles fonctionnalités sur helpdesk.

Par défaut, les nouvelles fonctionnalités optionnelles sont livrées en mode désactivé. Il est possible de les activer en émettant une demande auprès de l'interlocuteur Wittyfit Cegid privilégié, ou en activant les nouveaux droits ou la nouvelle configuration dans le logiciel.

Les équipes Produit de Cegid peuvent décider de distribuer, directement en production, des fonctionnalités très attendues ou des fonctionnalités qui amélioreront significativement l'utilisation ou le fonctionnement du logiciel. Dans ce cas, la documentation est transmise avant la mise en ligne ou une communication sur la plateforme est effectuée sous forme de tutoriel lors de la connexion à la plateforme.

Si, pour des raisons techniques, une fonctionnalité majeure ayant un impact sur l'ergonomie ou le fonctionnement de l'application doit être distribuée directement en production, la documentation correspondante est transmise avant la mise en ligne. Un rappel est envoyé deux mois avant la mise en ligne de la fonctionnalité.

3.2.2. Périodes de Maintenance

Le 1er mardi du mois :	18 h 30 - 19 h 30 CET patch management (version hebdomadaire, avec une courte interruption de production pour redémarrer l'application)
Bi-hebdomadaire :	Fenêtre de maintenance applicative avec interruption de services de quelques secondes.

Les maintenances planifiées sont communiquées, au minimum une semaine avant la date de maintenance, via le support, ou via notre canal de communication privilégié avec le client.

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 : **CODE ORANGE** ;
- incident de blocage généralisé ou situation dégradée : **CODE ROUGE** ;
- toutes les alertes de sécurité (connues ou potentielles) qui mettent en danger les données Client : **CODE NOIR**.

3.3.1. Aperçu du Processus de Gestion de Crise

La première action consiste à déclencher la création d'une « cellule de crise ».

Cette dernière identifie les Clients qui sont potentiellement impactés et établit un plan de communication afin d'informer les Clients impactés.

Dans le cas d'un code noir confirmé, la cellule de crise de Cegid est activée et gérée par le DPO et l'ISSM. La cellule identifie les Clients susceptibles d'être impactés et communique avec eux par l'intermédiaire des représentants qui ont été désignés dans la phase de projet comme représentants de la sécurité (ISSM ou équivalent).

Dans les autres situations (code rouge et code orange), la cellule de crise comprend, sans s'y limiter, le(s) consultant(s) en charge de l'incident, le manager de l'incident, les managers du service Clientèle, le représentant ISSM de Cegid ou un membre de son équipe, un représentant des services cloud et un représentant du service R&D. La cellule de crise fonctionne de la même manière que pour la gestion des incidents. Ainsi, des procédures de communication régulière, de résolution et de retour d'information post-crise sont mises en place.

La cellule est démantelée une fois le problème complètement résolu, les Clients informés de la résolution et le rapport d'incident créé. Le rapport d'incident comprend un résumé de l'incident, l'analyse avec la cause d'origine, les actions correctives et les éventuelles mesures préventives. La direction de Cegid réalise ensuite une analyse et un plan d'action d'amélioration (si nécessaire) en fonction des enseignements tirés des incidents.

Le processus de gestion de crise comprend des communications régulières à la direction de Cegid et à la direction exécutive si nécessaire.

3.4. Résiliation du Contrat

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 récupérer ses données accessibles au travers des fonctionnalités du Service ou demander à Cegid la restitution de ses Données. Cegid retransmettra 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 choisi par Cegid.

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 60 jours après la fin du contrat.

3.5. Demande de Services Supplémentaires

Une demande de service peut être faite en contactant votre représentant commercial ou votre interlocuteur Wittyfit Cegid privilégié.

Les prestations de service supplémentaires seront évaluées sur devis. Voici les services proposés :

- Session(s) de formation / Montées en compétences supplémentaire(s)
- Traduction des supports d'accompagnement dans des langues non proposées par Cegid Wittyfit
- Traduction de la plateforme Wittyfit en dans des langues non proposées par Cegid Wittyfit
- Installation et paramétrage d'un outil de lecture des questions
- Intervention ad hoc CSM / PS à la journée

4. SITES D'HEBERGEMENT

4.1. Lieux d'Hébergement

Cegid a choisi ses centres d'hébergement afin de permettre à ses Clients d'accéder à l'application Cegid Wittyfit et de respecter les réglementations en matière de confidentialité des donnée.

Zone géographique	Pays	Lieu principal (lieux secondaires)	Prestataire
Europe	France	France Marseille MAR02 (France Marseille MAR03) (France Lyon LYO03 pour les sauvegardes)	FreePro

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 fait de disposer de plusieurs centres nous permet d'être plus réactifs dans la mise en place de nouvelles instances Client, de gérer l'équilibrage de charge, de diminuer des risques, et d'augmenter notre capacité de manière rapide et indépendante.

Le fournisseur cloud et Cegid sont liés par un contrat qui comprend une clause de confidentialité. La liste des personnes autorisées à accéder aux données est revue régulièrement.

La structure juridique de Cegid est basée en France et les centres de données de Cegid Wittyfit sont situé en France (Marseille). Cegid garantit que la base de données est et sera toujours située 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. Pour plus d'informations, reportez-vous à la documentation suivante :

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

5. ARCHITECTURE TECHNIQUE

L'application Cegid Wittyfit 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 via une connexion SSL. 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 Wittyfit permettent :

- la séparation 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.

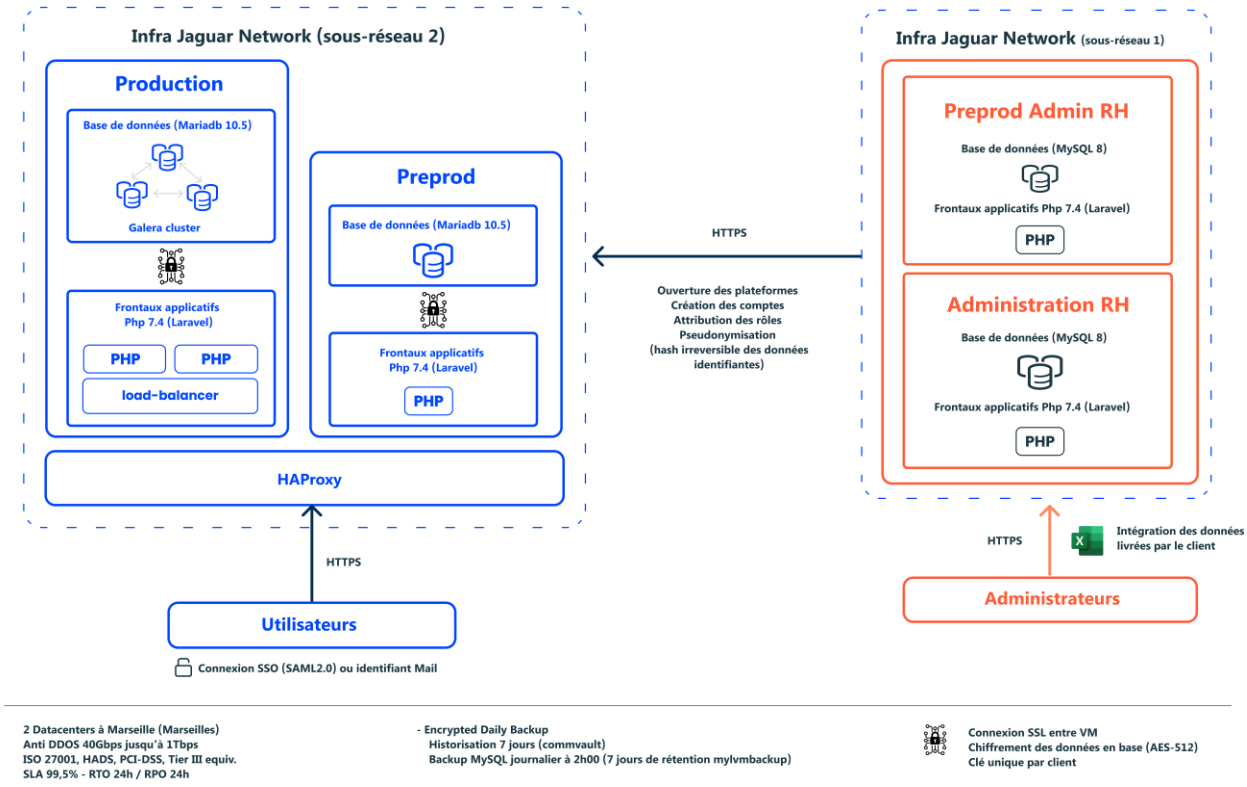
5.1. Architecture d'Application

La solution Cegid Wittyfit est composée de 2 plateformes séparé en sous-réseaux pour garantir l'anonymat des personnes :

- **Une plateforme utilisateur,** partie utilisée par les employés, les managers et les RH. Cette plateforme permet aux utilisateurs d'évaluer les différentes composantes de leur satisfaction au travail. Les managers et RH peuvent naviguer et analyser les résultats des différents groupes dans le temps et par entité, zone géographique (si défini) et filtre sociologique (si défini). Nous mettons en place une limite d'anonymat en dessous de laquelle les restitutions ne sont ni calculées, ni restituées. Cette limite peut être configuré à la hausse par le client, mais peut pas être inférieur à 5. La plateforme permet d'extraire des données au format Excell, power-point ou pdf.
- **Une Plateforme admin-RH,** partie principalement utilisé par les équipes d'intégration Cegid, et qui peut être mise à la main des équipes RH clients. Elle permet le chargement de la base utilisateur, l'attribution des droits managers, et la construction du filtre d'analyse sur la plateforme utilisateur. La synchronisation des données permet la pseudonymisation des comptes sur la plateforme utilisateur (hashage + salt) pour que les données émises par les utilisateurs ne puissent pas être reliées directement à leurs identifiants.

5.2. Architecture Serveur et Réseau

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



La technologie de virtualisation des serveurs applicatifs est VMWare. LA solution de backup de ses machines est Veeam.

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

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 Wittyfit autorisés, après une série de 2 filtres pare-feu et une séquence d'authentification forte. Chaque administrateur utilise un compte nommé et tracé (norme HDS).

Les serveurs de données sont inaccessibles depuis Internet. Seuls les serveurs applicatifs ont accès aux serveurs de données via connexion chiffrées au sein d'un cluster sous-réseaux isolé.

5.3. Infrastructure Technique de Logiciel

5.3.1. Composants d'Infrastructure

La solution tourne sur environnement LAMP. Elle se structure comme suit :

- au moins 2 Frontaux applicatifs PHP 7.4 (Laravel) + Python 3.11;
- bases de données (Mariadb 10.5, Redis) isolées / client (possibilité d'instancier un serveur dédié) ;
- application web basée sur Angular 9+, accessible uniquement en HTTPS.

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

Pour les modules PHP:

Composant	Produit	Version
Système d'exploitation serveur	Debian	10
Serveur Internet	Apaches	10.0
Cadre d'application	PHP	7.4
Moteur de base de données	Mariadb	10.5

Concernés : Administration RH, BO client, plateforme utilisateur

Pour les modules NodeJS:

Composant	Produit	Version
Système d'exploitation serveur	Debian	10
Serveur Internet	NodeJS	12.22.x
Cadre d'application	PM2	5.1.x
Moteur de base de données non relationnelle	Redis	6.0.16

Pour les modules Python:

Composant	Produit	Version
Système d'exploitation serveur	Debian	10
Serveur Internet	Python	3.10.10
Moteur de base de données non relationnelle	N/A	N/A

5.3.2. Bases de Données d'Application

L'application Cegid Wittyfit repose sur un groupe de bases de données :

Bases de données techniques qui ne contiennent pas de données Utilisateur

Base de données	Utilisation	Instances
Main-Core	Base de données qui répertorie tous les « locataires » d'un site physique + journaux techniques	Centralisée
RH-Core	Base qui répertorie tous les locataires pour l'admin-RH + journaux technique	Base de données accessible uniquement aux administrateurs techniques de Cegid

Bases de données contenant des données Utilisateur

Base de données	Utilisation	Instances
RH-Client	Base de données les listes d'utilisateur et leurs attributions à des groupes, la configuration des limitations à certains modules, et les affectations d'utilisateur à des groupes pour l'envoie de campagne de mail lié à l'activité de la plateforme.	Une base de données par Client
Main-Client	Base de données contenant la configuration des enquêtes du client, les données utilisateurs pseudonymisées, les agrégations de données par groupes, et les journaux techniques liés aux utilisateurs du client. Dans cette base de données les identifiants utilisateurs sont pseudonymisés sous forme de hash irreversibles.	Une base de données par Client

5.4. Gestion Multi-Clients

L'application Cegid Wittyfit est disponible sous forme de sites Web. Chaque Client possède son propre sous-domaine qui peut être desservi par une instance unique ou partagée du serveur Web. De cette façon, le produit possède une architecture logicielle multi-tenant et tous les sous-domaines pointent vers la dernière version de l'application. Chaque locataire dispose d'un domaine unique ou de quelques domaines uniques qui sont comparés à un identifiant unique de locataire.

Notre architecture est multi-tenant, la gestion multi-entités dans la couche de la base de données peut varier mais les serveurs applicatifs sont mutualisés.

Pour les bases de données principales (RH-Client, Main-Client) contenant la plupart des informations individuelles, l'architecture multi-tenant permet à ce que chaque Client dispose de sa propre base de données, co-hébergée sur des serveurs SQL partagés. Dans ce cas, le serveur Web se connectera à la base de données des locataires pour répondre à une demande. Les principales raisons de ce choix d'architecture sont les suivantes :

- gestion plus aisée de la sécurité et de la confidentialité des données ;
- sauvegardes et restaurations plus faciles ;
- possibilité de personnaliser le comportement de chaque instance d'application Client, même si le même produit est exécuté pour tous les Clients.

5.5. Environnement de Test

Une URL de test peut être mise à disposition de nos Clients en début de prestation pour valider avec notre équipe CSM la conformité du filtre, et la bonne prise en compte des indicateurs et questions par défaut.

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 de nouvelles fonctions avant qu'elles ne soient activées en production ou pour tester une action. Les données dans l'environnement de test sont une copie anonymisés des données de production à un moment donné et sont donc plus anciennes.

Par défaut, toutes les données d'une base de données de test sont anonymes et vide de tout contenu. Si le Client fait une demande de support, Cegid peut mettre à jour les données de test en utilisant les données de production en utilisant une méthode d'anonymisation des comptes (sans pièce jointe et avec un niveau d'anonymisation approprié).

Les Clients peuvent demander à Cegid de ne pas anonymiser les données dans un environnement de test. Toutefois, dans ce cas, les Clients sont responsables de la confidentialité des données et il faut s'attendre à un délai de livraison plus long.

Les environnements de test ne sont pas aussi disponibles que les zones de production. En outre, Cegid 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 Wittyfit est disponible sur deux plateformes mobiles : Android et iOS. L'application peut être téléchargée dans leurs bibliothèques d'applications respectives.

L'accès à l'application mobile peut se faire de la même manière que la version web. L'authentification unique est supportée à condition que le client ait mis en place un fournisseur d'identité.

L'application mobile Cegid Wittyfit ne fournit qu'une couche de présentation. Cela signifie qu'aucune donnée n'est stockée sur l'appareil mobile, à l'exception du cookie de connexion.

6. GESTION DES ACCES

6.1. Sécurité des Accès aux Applications

6.1.1. Plateforme utilisateurs

La plateforme utilisateurs accessibles via Internet en HTTPS. Le client choisi le sous-domaine par lequel ses utilisateurs y accéderont (ex: **societe**.witty.fit). L'utilisateur ou manager doit se connecter à la plateforme pour avoir accès au service.

6.1.2. Admin-RH

Accessible depuis internet, avec double-authentification par mail. Les accès aux données se fait selon le principe de moindre privilège.

6.2. Authentification

Par défaut, l'authentification à la plateforme Cegid Wittyfit se fait par la saisie d'un login et d'un mot de passe. La connexion SSO (SAML2) est disponible.

6.2.1. Responsabilités des Clients

Les Clients sont responsables de leur propre politique en matière de mots de passe. Cependant, nous vous informons que les politiques suivantes peuvent conduire à de graves infractions à la législation sur la protection de la vie privée (comme le RGPD) :

- réutilisation/clonage de mots de passe ;
- utilisation d'un algorithme pour construire les mots de passe ;
- utilisation d'un mot de passe connu par plus d'une personne ;
- utilisation de mots de passe divulgués ou de mots de passe « faciles à trouver » tels que « Admin1234 » ou « AZERty12@ » ;
- complexité inférieure à ce qui est recommandé par la CNIL : https://www.cnil.fr/fr/mots-de-passe-des-recommandations-de-securite-minimales-pour-les-entreprises-et-les-particuliers

Dans ce cas, seul le Client serait responsable de l'incident éventuel et de ses conséquences.

6.2.2. Plateforme utilisateur

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

- via le login et le mot de passe ;
- Via le mail de l'utilisateur
- par l'authentification unique (SSO SAML2).

Il est possible d'utiliser plusieurs méthodes d'authentification sur la même plateforme.

La session est entièrement gérée sur le serveur. Seul un cookie de session est stocké sur le poste de travail de l'Utilisateur.

6.2.3. Gestion des Mots de Passe

Règles par défaut pour les mots de passe (connexion email ou matricule):

Le mot de passe doit comporter au moins 8 caractères, et contenir:

- 1 majuscule
- 1 minuscule
- 1 chiffre
- 1 caractère spécial

Les mots de passe sont stockés en base hashés (argon2 + salage). Les identifiants de connexion sont également stockés hashés (SHA512 + salage)

A la demande du Client, Cegid Wittyfit peut être appliquer les politique de mot de passe suivante:

- Configuration à la hausse de la longeur de mot de passe
- Activation de la rotation du mot de passe
- Durée en semaine entre 2 modifications de mot de passe

La politique de mot de passe pour l'admin-RH impose 12 caractères, et une rotation du mot de passe tous les 3 mois.

Nous recommandons vivement l'utilisation de l'authentification unique (SSO) si le stockage des mots de passe dans une base de données pose problème.

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 :

- Dans le cas où l'identifiant est une adresse email, naviguer sur la page de login Cegid wittyfit pour renseigner son identifiant. Cliquer sur 'Mot de passe oublié'. Un email avec un code à 6 chiffres est envoyé sur l'adresse email de l'utilisateur. L'utilisateur doit renseigner ce code à 6 chiffres pour prouver qu'il est bien le détenteur de l'adresse email. L'utilisateur devra ensuite saisir un nouveau mot de passe avant de se reconnecter à l'application.
- Dans le cas de l'utilisation de matricule pour la connexion, naviguer sur la page de login de Cegid Wittyfit pour renseigner son identifiant. Cliquer sur 'Mot de passe oublié'. Choisir la question secrète choisie lors de l'activation du compte, et y répondre. L'utilisateur devra ensuite saisir un nouveau mot de passe avant de se reconnecter à l'application. Dans le cas où l'utilisateur aurait renseigné un email (optionnel) lors de la phase d'activation, le protocole précédent s'applique.

6.2.4. 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 (SSO) basée sur les protocoles SAML 2.0. Pour plus de détails, veuillez consulter la documentation publique des protocoles SAML 2.0.

6.2.5. Durée de la Session

La durée d'une session dépend de son utilisation particulière dans les différents modules de Cegid Wittyfit:

- Une session sur la plateforme utilisateur dure trente et un (31) jours.
- Une session sur l'admin RH est interrompue après soixante (60) minutes d'inactivité.

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, de maintenir la session de l'utilisateur et de leur permettre d'accéder à leurs comptes.

Pour obtenir la liste des cookies Cegid Wittyfit, veuillez-vous référer à : https://www.cegid.com/fr/politique-de-confidentialite/.

En ce qui concerne les données relatives aux cookies, Cegid 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.

6.4. Rôles, Droits et Habilitations

Cegid Wittyfit 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 Wittyfit. Les rôles sont fixes et définis, puis ils sont attribués aux Utilisateurs de Cegid Wittyfit. Les droits attribués aux rôles sont toutefois une liste définie dans le produit. Les rôles peuvent être restreint sur certains modules selon les besoins clients.

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 groupe. Une liste d'habilitation est une liste d'employés (appelés « managers »). Les managers ont ensuite accès aux résultats aggloméré du ou des groupes qu'ils managent (à la condition qu'il y est au moins 5 répondants dans la cohorte). Les habilitations peuvent être entièrement reconfigurées lors de l'import RH dans l'admin-RH Cegid Wittyfit.

Il est possible de générer automatiquement des listes d'habilitation d'Utilisateurs à partir de règles de gestion (en utilisant une organisation, par exemple). Ces listes sont automatiquement « actualisées ». Cela signifie que, si le contenu des organisations change, les listes seront automatiquement mises à jour, généralement sous quelques heures.

7. INTERFACES

Dans Cegid Wittyfit, il est possible d'exporter des données sous forme de fichiers au format CSV, XLSX, PPT ou PDF. L'import de la base utilisateur se fait par l'import d'un fichier CSV ou Excel. Ce chapitre décrit les principes qui sous-tendent les échanges de fichiers, 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. Principes de Fonctionnement

La solution Cegid Wittyfit permet l'importation de la base utilisateur depuis n'importe quel système capable de fournir un fichier CSV ou XLSX.

Pour que la synchronisation des données restent performante, nous limitons le service à une synchronisation bi-mensuel. Les importations peuvent être "différentielles" ou "complètes". Un intégrateur se charge de récupérer le fichier et de l'importer sur la plateforme admin-RH. Il vérifie ainsi le bon formatage et la cohérence globale des données.

L'accès à chaque importation est contrôlé par un droit d'accès et tracé dans l'interface d'administration.

L'équipe support Cegid met à la disposition de ses Clients une documentation complète sur la manière de construire le fichier au début du projet.

7.1.2. Vecteurs de transfert du fichier

Les Clients peuvent choisir la manière dont sera transmis le fichier.

- Cas de client non utilisateur de solution RH Cegid :

L'équipe Cegid Wittyfit met à disposition une boite de dépôt sécurisé (openTrust-MFT, chiffrement AES-256) permettant au client d'envoyer le fichier au support. Le fichier téléchargé est stocké dans un conteneur chiffré (VeraCrypt AES-256) sur disque chiffré avec Bitlocker. Le fichier est supprimé à la fin de la mise à jour.

Le Client peut mettre à disposition le fichier sur un quai SFTP et transmettre les accès à l'équipe technique pour mettre en place une automatisation de la récupération sécurisée de serveur à serveur. L'opérateur n'a pas directement accès au fichier, mais voit le résultat de l'import depuis l'interface d'admin-RH.

7.1.3. Liste des Formats d'Importation Disponibles

Le fichier peut être fournit en CSV ou XLSX. Cegid Wittyfit fournit une documentation complète sur la manière de construire le fichier au début du projet. Le format ne doit pas être modifier en cours de projet, ou nécessitera une reconfiguration de notre intégrateur.

7.2. Interface de messagerie

L'application Cegid Wittyfit envoie des emails en utilisant le protocole SMTP classique. Les emails peuvent être envoyés au format HTML ou au format texte brut lorsque les Clients ne peuvent pas traiter les emails HTML. Des mails automatiques sont envoyés pour la confirmation 2 facteurs lors de l'activation du compte ou lors du changement de mot de passe. Le contenu des mails est configurables lors du lancement de campagne ou la programmation d'évaluation d'action.

Les emails de de validation en 2 étapes proviennent du mail wittyfitsupport@cegid.com

Les emails de campagnes, évaluation d'actions et récapitulatif de l'activité pour les managers proviennent du mail noreply@wittyfit.com (aucun compte n'étant relié)

8. OPERATIONS

8.1. Procédures d'Exploitation

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

8.1.1. Purge

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.

Purge des fichiers téléchargé depuis SFTP sécurisé. Les fichiers stockés sur le serveur après échange SFTP sont stocké maximum trente et un (31) jours maximums.

8.1.2. Tâches Planifiées (tâches batch)

Un certain nombre de tâches batch sont prévues dans l'application standard (envoi d'emails, calcul des notifications, purges, mise à jour des coefficients).

Chaque tâche peut être lancée à l'aide d'un planificateur standard pouvant lancer une tâche de commande en ligne. Cegid est responsable de la gestion des planificateurs.

8.2. Management des Données

8.2.1. Sauvegarde des Données

Ce chapitre s'applique aux bases de données de production. Les bases de données de l'environnement de test ne sont pas sauvegardées.

Organisation des Sauvegardes

Les sauvegardes des bases 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.

La procédure standard prévoit que les sauvegardes soient sauvegardées sur des périodes glissantes en fonction de leur type :

Action	Fréquence de sauvegarde	Conservation des sauvegardes
Sauvegarde complète quotidienne des bases	Une fois par jour	Quatorze (14) jours
Snapshot des VM applicatives	Une fois par semaine	Quatorze (14) jours

Les supports de sauvegarde opéré pas le sous-traitant :

Action	Stockage de sauvegarde	Réplication des données
Privé (Jaguar Network)	VM	Les données sont répliquées au sein du même site primaire et exportées de manière asynchrone vers un centre de données secondaire.
Privé (Jaguar Network)	Disques de stockage	Les données sont répliquées de manière synchrone sur un centre de données distant.

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

Les données provenant des champs libre (idées, actions, sondages) sont chiffrées AES-256.

Données en transit

Cegid chiffre tous les transferts de données via le protocole HTTPS et TLS 1.2, et à travers la fourniture de certificats

Données au repos

Les identifiants et mots de passe sont sécurisés dans la base de données de manière non réversible grâce au hachage et au salage :

- en SHA512 +salt pour la gestion des identifiants ;
- en Argon2b + salt pour le stockage des mots de passe ;

En option gratuite, Cegid fournit une solution de cryptage des données textuelles dans le moteur de base de données (AES-256). Cependant, il faut noter qu'une réduction de 5 % des performances a été observée.

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 avec le sous-traitant. La supervision concerne :

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) ;

- surveillance de la disponibilité des applications ;
- surveillance du temps de réponse ;
- surveillance des tâches batch des applications et systèmes ;

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

- équipement physique (matériel de serveur, équipement de réseau, etc.) ;
- hyperviseurs ;
- réseau ;
- surveillance de la bande passante du réseau ;
- surveillance du matériel.
- surveillance de la charge de la plateforme (mémoire, processeurs, disques) ;
- mises à jour logicielles pour les systèmes d'exploitation, bases de données et antivirus ;
- 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

8.4.1. Plan de Reprise des Activités

- Les données Client sont répliquées en permanence dans deux centres de données distant de 5km à Marseille. Les backups journaliers sont conservés 14jours dans un datacenter situé à Lyon (69).
- Le processus de récupération est basé sur la réplication des données, la redondance de serveurs et l'automatisation de la restauration des services sur les datacenters infogérés par notre sous-traitant Jaguar Network (groupe freepro).

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 Wittyfit 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 Wittyfit, en tant que sous-traitant (Data processor), distingue deux personas différents : le salarié et le manager. 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. Pour des raisons de minimisation, les managers n'auront jamais accès en lecture aux données de cohorte de moins de 5 personnes (limite configurable à la hausse par le client)

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. Toutes les procédures relatives à la norme ISO 27001 sont en place. Ces procédures font partie de notre système de gestion de la sécurité de l'information.

Données sensibles

Cegid Wittyfit ne collecte pas de données sensibles, telles que celles mentionnées à l'article 9 du RGPD. Cegid Wittyfit 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. L'utilisation des espaces de champs libres est soumise à la lecture et acceptation d'une charte de bonne conduite, qui rappelle les précautions à prendre pour ne pas lever l'anonymat sur les personnes, ne pas transmettre d'informations confidentielles ou sensibles (données personnelles, business, opinion politique etc), et correspondre dans le respect de tous.

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 ISO 27001 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 Wittyfit 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 Wittyfit 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 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. L'utilisateur peut faire la demande à son DPO, ou utiliser la fonction d'effacement depuis son profil.

Il existe des conditions préalables à la suppression des données :

- La date de fin de contrat de l'ancien employé doit se situer dans le passé.
- Le dossier de l'employé doit être désactivé.

Bases légales

Le responsable de traitement a l'obligation de déterminer avant la mise en production de la solution Cegid Wittyfit 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.

9.1.3. Cartographie du traitement de données personnelles