cegid

Livret de Service

Cegid KMB Labs

01/09/2024

www.cegid.com

SOMMAIRE

cegid

cegid

cegid

HISTORIQUE DES MODIFICATIONS ET DES VALIDATIONS

Nature des modifications	Version	Date
Création du document	01	01/09/2024

Auditeur(s)

Date	Nom, fonction
01/09/2024	Alexandre Ragaleux, Directeur R&D
01/06/2024	Mathieu Lemonnier, Kévin Colleaux, Business Developpers

Approbateur(s)

Date	Nom, fonction
04/06/2024	Alexandre Ragaleux, Directeur R&D

Liste de distribution

Personne ou groupe
Client Cegid KMB Labs
Interne Cegid KMB Labs

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 KMB Labs.

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 ;
- RACI du support ;
- description de l'architecture technique de l'application Cegid KMB Labs, 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 Cegid KMB Labs.

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 KMB Labs sont basées en France (Boulogne-Billancourt). Les demandes de support peuvent être faites en français ou en anglais.

Les tickets de support doivent être émis à l'adresse suivante : support@kmblabs.com.

2.2. Contrat de Support

Cegid KMB Labs offre un support standard à tous ses produits. Pendant la phase de RUN, tous les tickets seront traités selon le principe du "Best Effort". Nous ne pouvons pas garantir un délai de traitement spécifique, mais nous mettons tout en œuvre pour les traiter le plus rapidement possible.

2.3. Section Support

Le support ne peut être fourni par Cegid qu'à condition que les administrateurs aient été formés de manière adéquate et soient autonomes dans l'utilisation de la solution.

Afin de faciliter l'exécution du Support, les administrateurs doivent, lors de la soumission des demandes, préciser les informations suivantes afin de permettre à Cegid de reproduire et de qualifier les éventuels incidents portés à sa connaissance :

- le type et la gravité de la demande ;
- une brève description du contexte ;
- les actions entreprises ayant mené à la génération de l'anomalie accompagnés d'une brève description du problème,
- une capture d'écran complète avec la date et l'heure de l'incident,
- Nombre et identité des utilisateurs impactés.

Les anomalies sont décrites dans la section 2.6.

Les demandes de configuration impliquent des actions techniques ou fonctionnelles que l'administrateur ne peut réaliser faute d'accès nécessaire.

Les tickets de type « question » sont toutes les demandes à caractère pédagogique ou résultant d'une requalification.

2.4. Définition Contractuelle des Anomalies et Politique de SLA

2.4.1. 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 rendant impossible l'exécution de tâches essentielles, entraînant une interruption des activités du client.
- 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.

2.4.2. SLA Standard Cegid pour Cegid KMB Labs

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 ouvrées	SLA en jours ouvrés
Bloquante	Vingt-quatre (15) heures	un jour et demi
Majeure	Cent (100) heures	Dix (10) jours
Mineure	Pas d'engagement – Best Effort	/

Les heures de travail de l'équipe du service Clientèle de Cegid KMB Labs sont du lundi au vendredi de 8 h 30 à 18 h 30.

Les accords de niveau de service (SLA) commencent dès que les incidents sont soumis via l'adresse support@kmblabs.com 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 « Provisoire » et « En attente d'approbation » 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 « Provisoire ».

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

2.4.3. Disponibilité du SaaS

Cegid s'engage à mesurer ses normes de service en dehors de ses périodes de maintenance programmées 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 ; hors défaillance des services tiers)

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 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 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.
- Comité d'examen opérationnel hebdomadaire avec les responsables du service clientèle et de la R&D

3.2. Procédure de Gestion des Changements

Régulièrement, Cegid effectue une mise à niveau de la version de Cegid KMB Labs 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.

Les nouvelles versions sont mises en ligne chaque semaine entre le lundi et le jeudi. Les clients ont le choix de passer sur la nouvelle version ou non.

3.2.1. Gestion de Versions

De nouvelles versions des applications Cegid KMB Labs sont publiées régulièrement. Dans certains cas, la mise à jour est obligatoire et profite à tous les clients. Dans d'autres cas, le déploiement de la nouvelle version est facultatif et peut être choisi par les clients en fonction de la valeur ajoutée qu'elle représente pour eux.

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.

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, un email sera envoyé au minimum une semaine avant la mise en ligne.

3.2.2. Périodes de Maintenance

Les maintenances ou les déploiements de mises à jour peuvent avoir lieu aux créneaux suivants :

Nuits du lundi au jeudi :	Minuit – 8h CET.
Le samedi matin :	2h - 4h CET (avec possibilité d'interruption de production)

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 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).

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, et au plus tard soixante jours à compter de la date de cessation des relations contractuelles, 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 en format texte .csv sans aucune altération de la structure logique de ces données.

Cegid s'engage à fournir au Client des informations sur la signification des colonnes et des liens entre les données des différents fichiers, afin de permettre au Client d'exploiter les données renvoyées.

Cegid 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.

- Dès réception de la demande du Client, une conférence téléphonique est organisée entre le Customer Success Manager, le Client ou son représentant, et le Service Client. Cette réunion a pour but de présenter le format de fichier de transfert de données et les procédures de transfert (SFTP/outil de transfert de fichiers du Client). Au cours de cette réunion, une date est planifiée pour le transfert de données.

- Une fois la date de transfert des données fixée, le Service Client fournit au Client les fichiers de transfert des données. Le Client accuse formellement réception de toutes les données. Après la réception, Cegid ferme la version de l'application du Client et détruit toutes les sauvegardes.
- Le Service Client fournit au Client un certificat de destruction.

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 irrémédiablement toutes les données Client (y compris la base de données, l'URL et les sauvegardes). Sur demande, Cegid fournira aux Clients une déclaration de destruction des données.

3.5. Demande de Services Supplémentaires

3.5.1. Services supplémentaires

Le Client peut, à tout moment, émettre une demande de services supplémentaires. Cette demande se fait par l'intermédiaire du Customer Success Manager/responsable de compte. Cegid fournit le devis correspondant dans les quinze (15) jours ouvrables.

Pour les demandes plus complexes, une conférence téléphonique peut être programmée avec l'équipe Services avant de remettre le devis au Client.

3.5.2. Offre par crédits TJM

Dans le cadre du support fourni par le Cegid-KMB Labs Customer Care, certaines actions sortent du cadre du support standard que nous pouvons vous offrir.

Ces actions peuvent être réalisées dans le cadre de crédits TJM (Tarif Journalier Moyen). Les services avancés sont d'une durée minimale d'une journée.

Un service peut nécessiter plusieurs crédits. Le service est réalisé par des consultants fonctionnels ou techniques. Vous pouvez souscrire à un paquet de jours. Les crédits de service via paquets de jours sont vendus par jour et peuvent être utilisés par jour ou par heure.

Si vous disposez déjà de crédits TJM et que votre demande sort du cadre du support standard, le consultant du Service Clientèle vous indiquera que votre demande peut être réalisée dans le cadre d'un service basé sur les crédits, nécessitant l'utilisation de 'x' crédits. Dès que vous aurez validé, le service pourra être exécuté.

Si vous ne disposez pas de crédits de service, vous pouvez contacter votre représentant commercial ou CSM pour plus d'informations.

3.5.3. Comités de suivi

Fréquence : une fois par trimestre (en fonction du périmètre fonctionnel)

Objectifs :

- **Faciliter votre administration courante**

  En créant une relation de proximité et un suivi régulier avec les administrateurs

- **Prendre en charge vos besoins spécifiques**

En approfondissant les investigations nécessaires sur vos tickets

- **Être garant de la relation auprès des équipes techniques et des partenaires technologiques**

En apportant des éléments contextuels à vos demandes

Participants :

- Cegid : consultant.s dédié.s
- Client : administrateur.s central.aux

3.5.4. Comité de Pilotage

Fréquence : une fois par an (en fonction du périmètre fonctionnel)

Objectifs :

- **Contribuer à vos enjeux stratégiques**

En animant des comités de pilotage en analysant les périodes passées et en planifiant les actions majeures

- **Partager la vision de KMB Labs**

En partageant des informations sur les produits ou actualités diverses

- **Engager l'ensemble de l'écosystème**
- **Piloter la qualité de service selon vos enjeux RH**

En facilitant la prise de décision, et le suivi de plans d'action opérationnels

Participants :

- Cegid : consultant.s dédié.s (fonctionnel et/ou technique), Customer Success Manager, responsable de compte
- Client : administrateur central, key users

3.5.5. Ateliers

Fréquence : Nombre de jours défini en fonction du scope fonctionnel couvert par la solution et à consommer dans les 12 mois.

Objectifs :

- **Présentation de nouvelles fonctionnalités dans le contexte du client (sur les modules déployés)**
- **Focus sur une fonctionnalité particulière / Prise en main**
- **Partage de bonnes pratiques**
- **Propositions d'optimisation de configurations (techniques ou fonctionnelles)**

Participants :

- Cegid : consultant.s dédié.s (fonctionnel et/ou technique)
- Client : administrateurs, key users

4. SITES D'HEBERGEMENT

4.1. Lieux d'Hébergement

Cegid dispose actuellement de plusieurs centres de données dans le monde entier afin de permettre à ses Clients d'accéder à l'application Cegid KMB Labs et de respecter les réglementations en matière de confidentialité des données dans leur pays d'origine.

Zone géographique	Pays	Lieu principal (lieu secondaire)	Prestataire
Europe	Irlande	Dublin	Amazon Web Services
Europe	France	Europe du Nord - Dublin (Europe de l'Ouest - Amsterdam)	Microsoft Azure Europe du Nord
Europe	France	Allemagne centre-ouest - Francfort (Allemagne nord - Berlin)	Google Cloud Platform

4.2. Sécurité et Confidentialité des Prestataires d'Hébergement

Nous, Cegid, évaluons et sélectionnons les centres d'hébergement selon des critères stricts de sécurité, de confidentialité, de qualité et de disponibilité. Le fait de disposer de plusieurs centres nous, Cegid, permet d'être plus réactifs dans la mise en place de nouvelles instances Client, de partager les risques et les charges de travail entre plusieurs prestataires, 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 KMB Labs pour les Clients européens sont basés dans l'Union européenne (y compris la France). 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.

Cegid peut donc garantir une protection complète contre le US Patriot Act à tous les Clients qui souhaitent s'en protéger.

Les centres d'hébergement de Cegid 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 :

- Microsoft Azure : https://learn.microsoft.com/en-us/compliance/regulatory/offering-home
- Amazon Web Services : https://www.ovhcloud.com/fr/enterprise/certification-conformity/
- Google Cloud Platform : https://www.ibm.com/cloud/compliance/global

5. ARCHITECTURE TECHNIQUE

L'application Cegid KMB Labs 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 et autres services de traitement 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 KMB Labs 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.

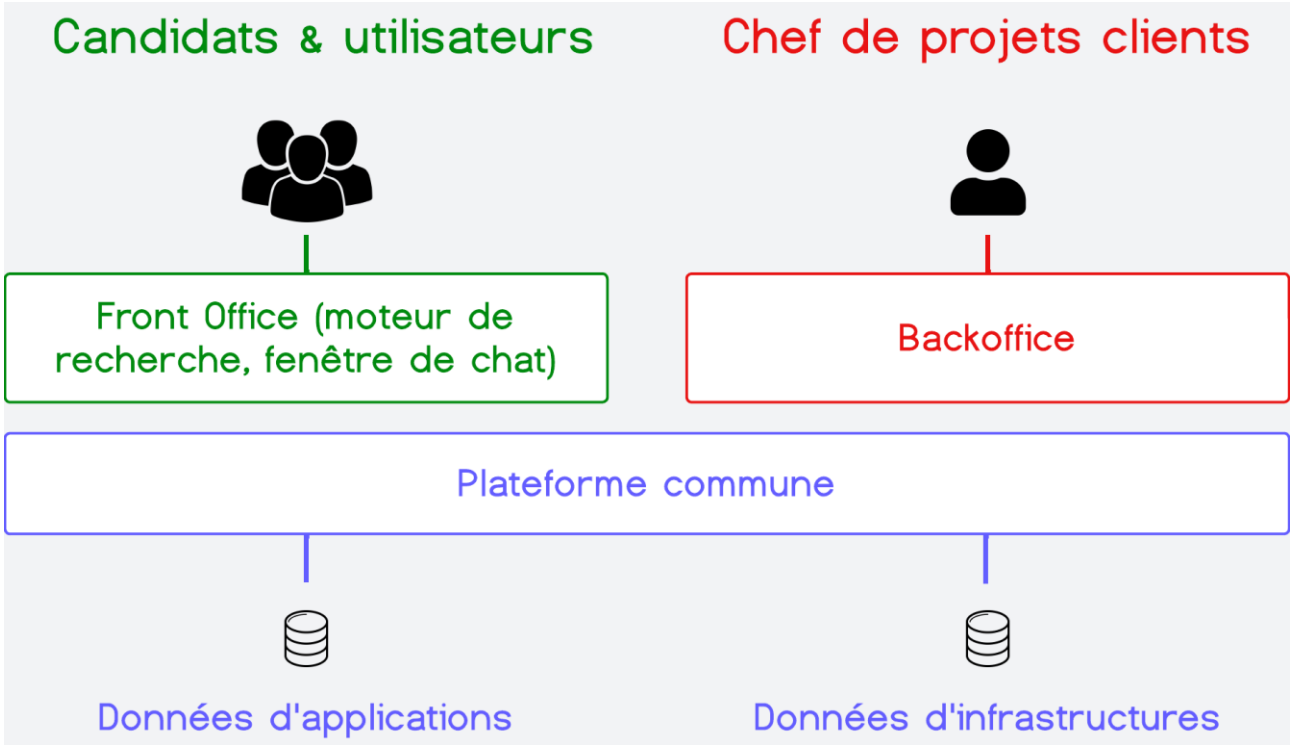
Bien que l'architecture de Cegid KMB Labs permette de nombreuses options, certaines d'entre elles ne sont pas disponibles lorsque l'on utilise les méthodologies de projets selon nos offres, et certaines ne sont pas non plus disponibles en fonction du périmètre fonctionnel. Ces méthodologies reposent sur un temps d'exécution court et la réutilisation de paramètres par défaut pour la plupart des aspects de la solution.

5.1. Architecture d'Application

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

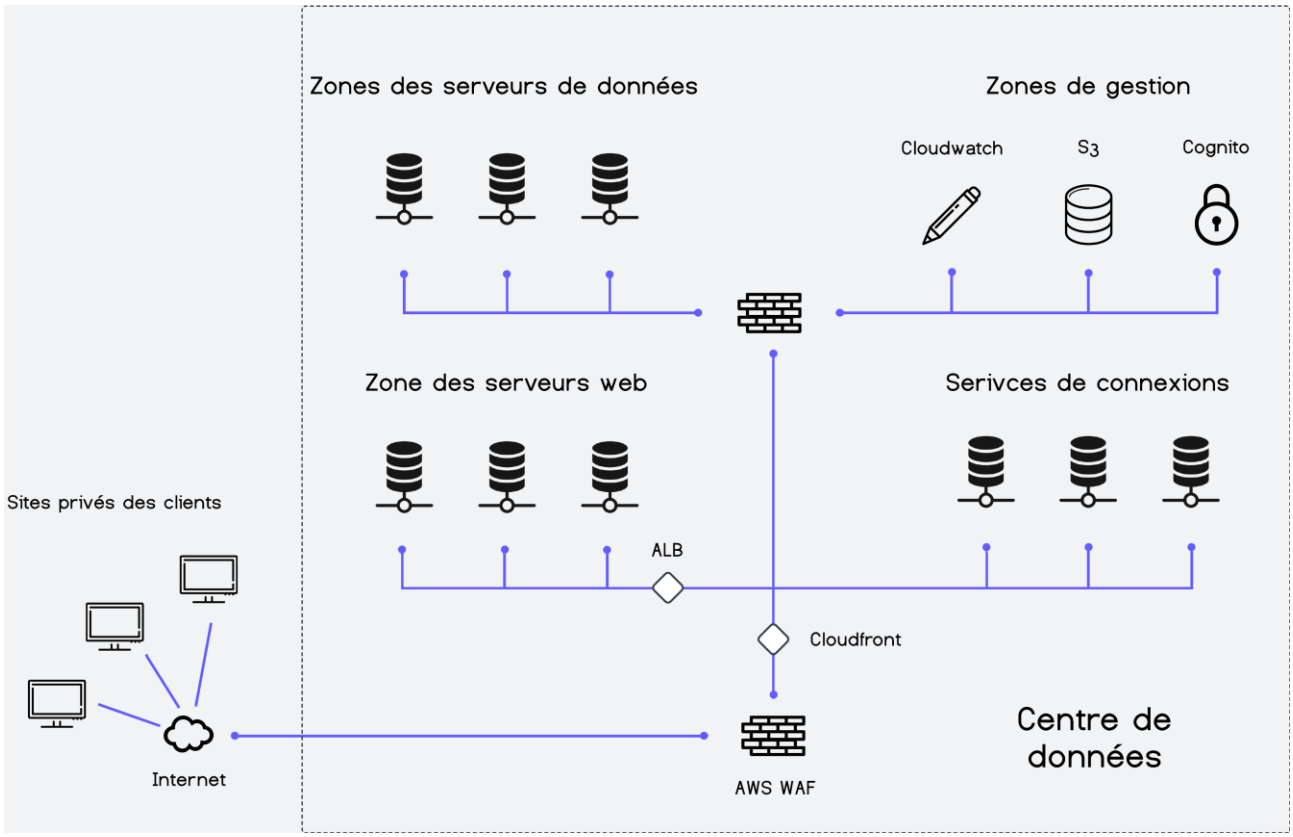
- Un Backoffice. Cette partie est principalement utilisée par les équipes RH. Le Backoffice est utilisé pour tous les processus de gestion des produits KMB Labs : chatbots, Moteurs de recherche Conversationnel, configuration WhatsApp, Statistiques, etc...
- Un ou plusieurs Front Office(s). Les Front Offices permettent aux utilisateurs d'échanger avec les chatbots et d'utiliser les moteurs de recherche. Il est possible d'exécuter plusieurs Front Offices qui correspondent à plusieurs portails Internet, chacun ayant des fonctionnalités et des chartes graphiques différentes. Les Front Office(s) comprennent également les canaux de discussions de services tiers (WhatsApp, Facebook Messenger, ...).
- Toutes les informations peuvent être constituées au sein d'une ou plusieurs bases de données.

Le Front Office est un bloc indépendant car il est exposé à l'Internet public. Il est toutefois relié à un Back Office afin de personnaliser les produit, et consulter les métriques clés.



5.2. Architecture Serveur et Réseau

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



cegid

La technologie de virtualisation utilisée dépend du centre de données : AWS Nitro est actuellement utilisé dans notre service cloudAWS, tandis que nos fonctionnalités hébergées sur le cloud Azure sont basées sur des machines virtuelles Azure.

Les serveurs Web disposent tous de systèmes sophistiqués de répartition de charge. Quant aux serveurs de bases de données, ils sont équipés de mécanismes de sauvegarde permettant une restauration ultra-précise, à la seconde près (PITR - Point In Time Recovery).

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 KMB Labs autorisés, après une séquence d'authentification forte. Chaque administrateur utilise un compte nommé.

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

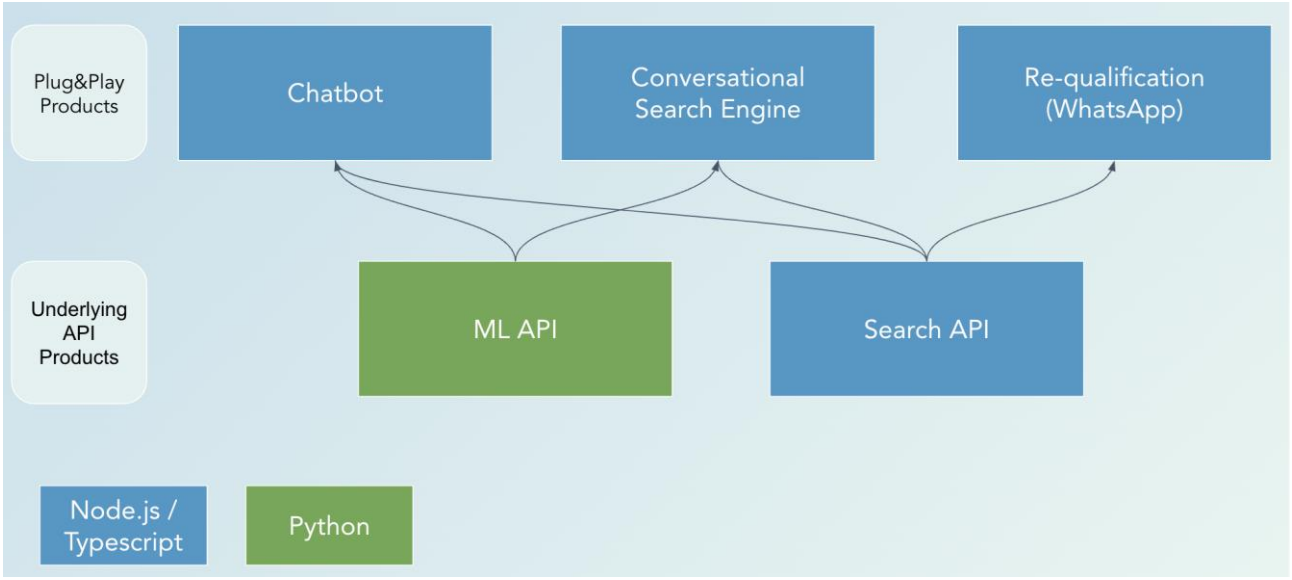
5.3. Infrastructure Technique de Logiciel

5.3.1. Composants d'Infrastructure

Nos produits sont conçus avec les langagesNode.js/Typescript, sauf pour notre webservice « Machine Learning » qui est écrit en Python. L'intégralité de notre architecture s'appuie sur une utilisation de plusieurs services AWS (AWS Lambda, AWS WAF, AWS CloudFront, AWS Api Gateway…).

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

Notre architecture de Cegid KMB Labs est disponible uniquement en mode SaaS.



5.3.2. Bases de Données d'Application

Une application Cegid KMB Labs repose sur un groupe de bases de données :

Les bases de données utilisées sont les suivantes :

Base de données	Utilisation	Instances
BO-Projects	Base de données contenant le paramétrage des produits KMB Labs à travers le Back Office. Cette base de données ne contient aucune donnée personnelle ni de données sensibles.	DynamoDB, Mutualisé
Client-Data	Base de données contenant principalement les données structurées d'un client (offres d'emploi). Elle est utilisée par nos APIs de recherche (Search API) afin de trouver les bonnes offres d'emploi aux candidats.	Une base de données par Client. PostgreSQL avec réplication sur ElasticSearch.
User-Sessions	Utilisées pour enregistrées les informations de sessions d'un utilisateur. Produit chatbot uniquement.	Une base de données par Client. MongoDB avec réplication sur Redis.
Data-Embeddings	Base de données contenant les documents vectorisés (ou embeddings) des clients.	Mutualisé. PostgreSQL avec PGVector.
Data-File	Datastore contenant toutes les pièces jointes (fichiers)	AWS S3.

5.4. Gestion Multi-Clients

L'application Cegid KMB Labs est disponible sous forme de sites Web.

En dehors du Back Office, qui est une architecture commune à tous nos clients, chaque Client possède son propre sous-domaine qui est desservi par une instance / unités de calculs spécifiques.

Bien que l'architecture du produit soit purement multi-tenant dans tous les cas dans la couche du serveur Web (logiciel), la gestion multi-entités dans la couche de la base de données peut varier, avec différents modèles utilisés selon le produit.

Pour les bases de données principales (Client-Data, User-Sessions, Data-File) contenant la plupart des informations individuelles, l'architecture multi-tenant est très limitée car chaque Client dispose de sa propre base de données, co-hébergée sur des serveurs 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.

Cependant, pour les bases de données BO-Projects, Data-Emebeddings, l'architecture est différente et plusieurs Clients peuvent partager la même base de données. Dans ce cas, le serveur Web se connectera à la même base de données pour de nombreux Clients et le composant logiciel responsable de l'isolation des locataires limitera toutes les demandes à la base de données aux données des locataires.

En outre, toutes les données enregistrées par KMB Labs sont chiffrées.

5.5. Environnement de Test

Chaque Client dispose d'une URL de production et d'une URL 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 de nouvelles fonctions avant qu'elles ne soient activées en production ou pour tester une action.

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

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).

D'autres environnements peuvent également être ajoutés, par exemple : un deuxième environnement de test, un environnement de formation, etc. La mise en œuvre de ce service peut faire l'objet d'un accord commercial supplémentaire.

5.6. Reporting/Analyse

Tous les produits partagent une fonction de reporting permettant la gestion des rapports, soit directement dans l'interface Utilisateur, soit en générant des fichiers CSV, Excel ou PDF selon le rapport.

Les fonctions analytiques sont fournies par une infrastructure « producters / consumers » via AWS Kinesis et AWS RDS pour l'enregistrement des métriques. Cette infrastructure est multi-tenant et chaque Client dispose de ses propres métriques dans un moteur partagé. Les données analytiques sont conservées dans le même centre de données que les données opérationnelles. Cegid se conforme aux réglementations locales en matière de protection des données de la même manière pour les données analytiques et opérationnelles.

Les rapports sont accessibles depuis l'application en fonction des droits accordés à l'Utilisateur connecté. Ils peuvent également être envoyés par mail aux personnes ayant accès à l'administration des solutions KMB Labs sur le Back Office.

6. GESTION DES ACCES

6.1. Sécurité des Accès aux Applications

6.1.1. Front Office Candidat

Par définition, les applications « Chatbot » et « Moteur de Recherche » sont exposées et accessibles via Internet.

6.1.2. Back Office

Plusieurs méthodes d'accès sont possibles :

- Application exposée et librement accessible via Internet ;
- L'accès à l'application peut être limité à des groupes spécifiques d'adresses IP. Tous les accès en dehors de ce groupe défini d'adresses IP seront interdits.

6.2. Authentification

Par défaut, l'authentification sur le Back Office de Cegid KMB Labs sse fait par la saisie d'un login et d'un mot de passe.

Voici la politique de mot de passe :

- Douze (12) caractères minimums
- Un (1) chiffre minimum
- Un (1) caractère spécial minimum
- Un (1) caractère minuscule minimum
- Un (1) caractère majuscule minimum

6.2.1. Responsabilités des Clients

Nous 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 « @dmiN123456789 » ou « AZERty12345678@ » ;
- Dans ce cas, seul le Client serait responsable de l'incident éventuel et de ses conséquences.

6.2.2. Détails de l'Authentification

Il n'est pas possible de s'inscrire sur le Back Office KMB Labs sans invitation. Les invitations peuvent être envoyés par :

- L'équipe Cegid KMB Labs qui va être responsable d'initialiser le projet
- Les utilisateurs déjà inscrits avec le rôle de « Manager » sur au moins un des projets auquel ils ont accès.

Un mail d'invitation est donc envoyé contenant :

- L'identifiant unique de l'utilisateur ;
- Le mot de passe temporaire de l'utilisateur

Ces deux informations doivent être renseignées sur le Back Office KMB Labs à la première connexion. L'utilisateur se verra alors demandé de renseigner un nouveau de mot de passe pour son compte.

Le MFA est également également disponible sur demande (via SMS). Dans ce cas, les numéros de téléphones des utilisateurs concernés devront être fournis à l'équipe KMB Labs par mail (support@kmblabs.com).

La session est entièrement gérée côté serveur, via AWS Cognito. 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.

Mots de passe perdus/oubliés. Lorsque les Utilisateurs oublient leur mot de passe, ils doivent procéder comme suit :

- Utiliser un navigateur Internet pour accéder à leur page de connexion Back Office Cegid KMB Labs ;
- Saisir le login dans le champ « Vous avez oublié votre mot de passe », puis cliquer sur « ENVOYER » ;
- 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.

6.2.3. Durée de la Session

La durée de la session est de douze heures (cela peut être modifié en fonction de la configuration).

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 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.

6.3. Rôles, Droits et Habilitations

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

6.3.1. Rôles et Droits

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

7. INTERFACES

Dans Cegid KMB Labs, il est possible d'importer et d'exporter des données sous forme de documents de divers formats (csv, txt, docx, ppt, etc.) 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. Stockage et traitement des documents

7.1.1. Gestion des fichiers dans l'interface Back Office

Les documents importés dans Cegid KMB Labs sont stockés de manière sécurisée sur AWS S3. Une fois enregistrés, ces documents subissent un traitement spécifique visant à les rendre exploitables par l'intelligence artificielle du système. Ce traitement consiste à découper le contenu des documents et à le transformer en "Vecteurs". Ces vecteurs permettent à l'IA de retrouver efficacement les informations pertinentes lors des requêtes.

7.1.2. Gestion des fichiers dans les interfaces Front Office

Les utilisateurs des solutions chatbots et moteur de recherche ont la possibilité d'uploader des fichiers directement via les interfaces Front Office "Chatbot" et "Moteur de recherche". Dans le cas spécifique des CV, un traitement particulier est appliqué :

1. Analyse des CV : Les CV uploadés sont analysés par un prestataire externe avec lequel le client a déjà établi un contrat (comme TextKernel ou Xtramile).

2. Transformation en données structurées : L'analyse permet de convertir le CV en un format de données structurées (JSON).

3. Utilisation pour le matching : Ces données structurées sont ensuite utilisées pour effectuer un matching entre les profils des utilisateurs et les offres d'emploi disponibles.

4. Durée de conservation limitée : Il est important de noter que ni les CV originaux, ni les CV analysés ne sont conservés après ce traitement. La durée maximale de stockage de ces documents est limitée à 1 minute, assurant ainsi une gestion responsable et conforme des données personnelles.

Cette approche permet d'optimiser le processus de recrutement tout en respectant les principes de protection des données et de minimisation de la conservation des informations personnelles.

7.2. Sécurité des données

La sécurité des données est une priorité absolue. Toutes les informations sont chiffrées, aussi bien lors de leur transfert (chiffrement en transit) que pendant leur stockage (chiffrement au repos). Cette approche garantit la confidentialité et l'intégrité des données à chaque étape du processus.

7.3. Interface SFTP Sécurisée et Webservices

Le Client peut nous transférer des données via notre serveur SFTP sécurisé – par échange de clés publiques ou par mot de passe.

L’opération inverse est également possible : KMB Labs eput récupérer les données d’un Client sur leur serveur SFTP ou webservices externes. Cegid KMB Labs se charge d’opérer toutes les configurations nécessaires. Ce service peut être indisponible selon l’offre souscrite.

7.4. Interface de messagerie

L'application Cegid KMB Labs envoie des emails en utilisant le service Mailgun ou AWS SMS. Les emails peuvent être envoyés au format HTML ou au format texte brut lorsque les Clients ne peuvent pas traiter les emails HTML.

Par défaut, les applications utilisent l'adresse expéditeur @kmblabs.com. Si vous souhaitez modifier votre adresse email d'expéditeur, veuillez nous contacter.

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 est conservé pendant quatre-vingt-dix (90) jours, les données plus anciennes sont purgées. Cette durée est paramétrable, pour cela veuillez nous contacter.

Purge des fichiers stockés sur FTP sécurisé. Les fichiers stockés sur le site FTP sécurisé sont conservés pendant quatre-vingt-dix (90) jours maximum.

8.1.2. Tâches Planifiées (tâches batch)

Un certain nombre de tâches batch sont prévues dans l'application standard (envoi d'emails, indexation de données...).

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.

Actions d'exploitation spécifiques. Cegid permet de planifier des actions spécifiques dans l'environnement de production et de test d'un Client, à la demande de ce dernier. Cependant, toute demande est soumise à l'approbation de Cegid.

8.2. Management de la Donnée

8.2.1. Sauvegarde des Données

Ce chapitre s'applique à toutes nos bases de données.

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 réalisées sur des périodes glissantes en fonction de leur type :

Action	Fréquence de sauvegarde	Conservation des sauvegardes
Sauvegarde complète quotidienne	Une fois par jour	Trente (30) jours
Sauvegarde complète mensuelle	Une fois par mois	Douze (12) mois

Les supports et emplacements de sauvegarde dépendent du fournisseur cloud :

Action	Stockage de sauvegarde	Réplication des données
Azure	Conteneur Azure Blob	Les données sont répliquées au sein du même site primaire et exportées de manière asynchrone vers un centre de données secondaire.
AWS	AWS S3	Les données sont répliquées au sein du même site primaire et exportées de manière asynchrone vers un centre de données secondaire.

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 et au repos

Toutes les données reçues par KMB Labs sont transmises via Secure Sockets Layer (TLSv1.2+ sur HTTPS ou SCP) aux serveurs de KMB Labs et chiffrées à l'aide d'algorithmes de chiffrement de haut niveau (AES256, AES512, AES1024).

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.

L'outil utilisé pour la supervision des infrastructures et des applications est AWS CloudWatch / AWS CloudTrail.

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.

Pour plus de détails, veuillez-vous référer aux documents « Shared-responsability Model » d'Azure et AWS.

8.4. Plan de Continuité des Activités

Chez Cegid KMB Labs, nous comprenons la nature critique de ces opérations et l'impact potentiel des perturbations. Notre engagement à assurer une continuité d'activité robuste et un processus de reprise après sinistre rapide se reflète dans nos plans de DR et de BC bien définis.

8.4.1. Aperçu des plans DR et BC

8.4.1.1. Plan de reprise après sinistre informatique (DR)

Notre plan DR est axé sur la restauration des systèmes et services informatiques après toute perturbation. Cela comprend :

- Sauvegardes et restauration des données
- Récupération des logiciels et applications critiques
- Restauration du matériel et de l'infrastructure

8.4.1.2. Plan de continuité d'activité (BC)

Le plan BC assure le flux ininterrompu des opérations commerciales critiques même face à des événements imprévus. Cela comprend :

- Processus opérationnels alternatifs
- Gestion et réaffectation de la main-d'œuvre
- Stratégies de communication avec les parties prenantes

Objectif de temps de reprise (RTO) et objectif de point de reprise (RPO)

Pour le succès de nos plans DR et BC, il est crucial d'avoir des objectifs clairs qui répondent aux attentes de l'entreprise :

- Objectif de temps de reprise (RTO) : C'est le temps maximal autorisé pour la restauration des systèmes et applications après une perturbation. Pour Cegid KMB Labs, le RTO défini est de 24 heures. Cela signifie qu'en cas de perturbation, nos systèmes informatiques et applications critiques seront opérationnels dans les 24 heures.
- Objectif de point de reprise (RPO) : Il représente la quantité maximale acceptable de perte de données mesurée en temps. Il détermine la fréquence à laquelle les sauvegardes doivent être effectuées. Chez Cegid KMB Labs, notre RPO s'aligne sur nos stratégies de sauvegarde fréquentes assurant une perte de données minimale.

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 KMB Labs.

Important : tous les éléments de sécurité des données sont décrits dans notre Politique de 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 KMB Labs, 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 KMB Labs ne collecte pas de données sensibles, telles que celles mentionnées à l'article 9 du RGPD. Cegid KMB Labs 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 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 KMB Labs 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 KMB Labs 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.

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 disposant d'un compte Cegid KMB Labs peuvent supprimer ou rectifier leurs données personnelles par demande par courriel à l'adresse support@kmblabs.com.
Les candidats peuvent demander l'exportation de leurs données personnelles. Ils recevront un courriel contenant un lien pour télécharger un fichier zip contenant toutes leurs données personnelles.

Droit à l'oubli

Toutes les données des candidats ou des utilisateurs de nos produits « Chatbot », « Moteur de Recherche » et « WhatsApp » voient leurs données personnelles supprimées ou anonymisées après un maximum de quatre-vingt-dix (90) jours.

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

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

9.2. Référentiel Général d'Amélioration de l'Accessibilité – RGAA

CEGID s'engage dans une démarche de mise en accessibilité de ses services et produits numériques conformément à l'article 47 de la loi n°2005-102 du 11 février 2005.