Livret Service

Cegid Wittyfit

Version Février 2023

cegid

SOMMAIRE

Table des matières

Table des matières

Préambule

Ce document a pour vocation de résumer de manière synthétique nos différents services autour de l'hébergement, la sécurité et nos niveaux d'engagement. Chacun de ses éléments peut être approfondi à la demande de nos clients.

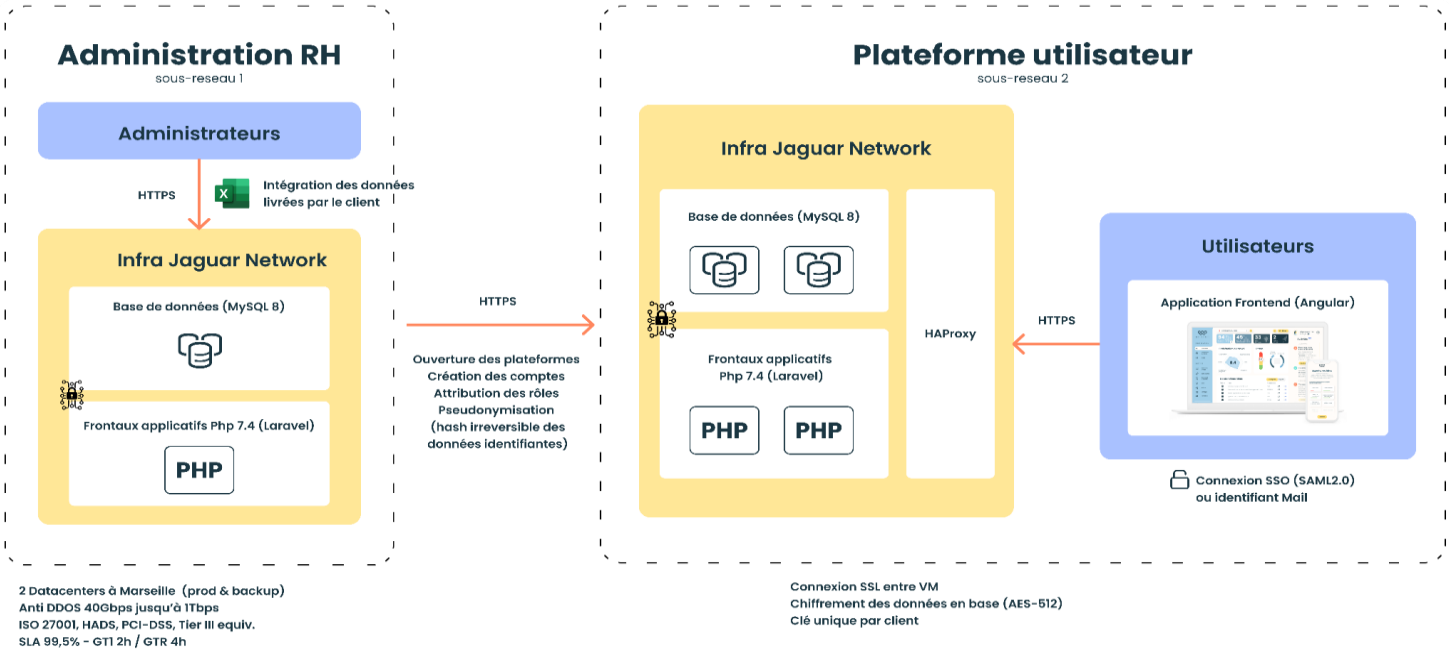
Notre infrastructure

Architecture technique

Notre infrastructure est hébergée chez Jaguar Network, composé de 2 sous-réseaux étanches qui cloisonnent d'un côté l'administration RH et de l'autre pour l'application Cegid WITTYFIT et son administration technique. Notre solution tourne sur environnement LAMP

Elle se structure comme suit :

- au moins 2 Frontaux applicatifs PHP 7.4 (Laravel)
- Bases de données (MySQL 8, Redis) isolées / client (possibilité d'instancier un serveur dédié)
- Application web basée sur Angular 9+, accessible uniquement en HTTPS
- Sauvegardes toutes les nuits 2h + Image serveur hebdomadaire



Le HAProxy nous permet de mettre en place des règles spécifiques de redirection pour nous conformer à des exigences clients (ex: restriction IP), ou organisation interne. Les frontaux applicatifs sont virtualisés, un système de load-balancer nous garantit une prise en charge en cas de pic d'utilisation ponctuelle, et l'hébergeur peut mettre en place rapidement de nouvelles instances en cas de montée en charge plus longue.

Gestion de la confidentialité des données et de la pseudonymisation des comptes

La confidentialité des données de nos utilisateurs est l'un des facteurs clé de l'adhésion des salariés à l'outil, et par conséquent à la démarche globale. Cegid Wittyfit a intégré la protection des données dès la conception du produit et dès ses premières lignes de code. Ainsi, conformément au RGPD et à la logique d'"accountability", Cegid Wittyfit respecte le "privacy by design".

En outre, afin de pouvoir travailler en partenariat avec le CHU de Clermont-Ferrand, nous avons dû répondre aux critères posés par son comité d'éthique – en sus de ceux du RGPD – en termes de protection des données. Enfin, nos données sont hébergées en France et chez un Hébergeur Autorisé Données de Santé (HADS).

Cegid Wittyfit garantit à ses utilisateurs et co-contractants, les mesures maximales en termes de protection des données. Nous mettons bien sûr à votre disposition tous les documents nécessaires à la réalisation du PIA – Privacy Impact Assessment.

Cegid Wittyfit est garant de la confidentialité des utilisateurs tant lors du traitement des données que lors des restitutions.

C'est pourquoi nous séparons notre application en 2 plateformes. L'une pour la gestion des comptes, à la main d'un opérateur, qui à partir de la liste des utilisateurs autorisés, autorise la création de compte et active les autorisation pour chaque compte. Cette plateforme (Admin-RH) est dissociée de la plateforme de recueil des ressentis utilisateurs (sous-réseau séparé), et pilote la création des comptes après pseudonymisation.

Lors de la création des comptes :

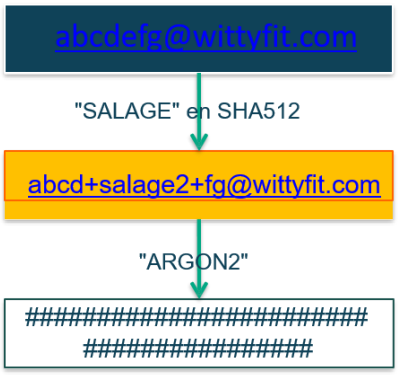
Pour le transfert des données initiales de création de comptes et l'attribution des rôles, nous fournissons au client une boîte de dépôt sécurisée chiffrée (solution opentrust MFT, chiffrement AES-256) pour le transfert des données. Un mail chiffré de la part du client peut être utilisé. Le stockage temporaire se fait dans un container chiffré via Veracrypt (AES-512) le temps de l'opération.

La plateforme d'administration est accessible via une authentification forte à 2 facteurs avec rotation des mots de passe.

Lors du traitement des données :

Les emails des collaborateurs "subissent" un chiffrement salé, il ne peut y avoir d'identification directe La seule donnée identifiante fournie par l'entreprise n'est pas stockée dans la base de données, elle est remplacée par un chiffrement non réversible :

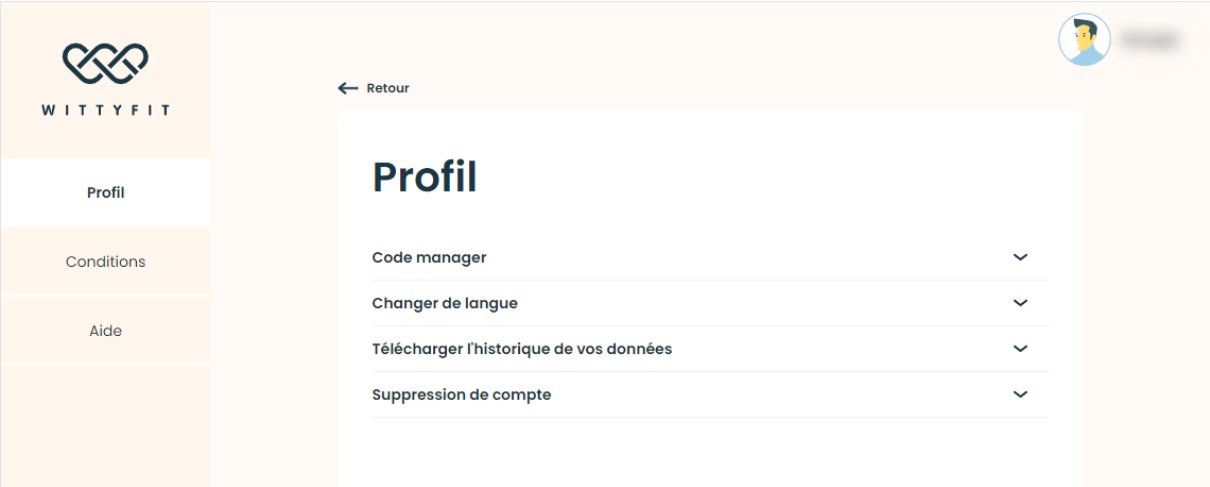
>abcd@wittyfit.fr + salage puis sha512
>mot de passe + salage2 puis argon2



Lors des restitutions dans notre plateforme :

Les résultats d'un groupe ne s'affichent que si, a minima, 5 personnes de ce groupe se sont exprimées. Ainsi, aucune donnée n'est accessible en dessous de 5 répondants. Seuls les utilisateurs connectés avec

leur propre compte peuvent avoir accès aux données qu'ils ont renseigné, soit en naviguant sur les différents questionnaires, soit en demandant le téléchargement de l'historique des données depuis le menu paramètre.



Modes de connexion

Les modalités de connexion au service sont doubles :

- Identifiant mail ou matricule RH
- SSO via SAML2

Les identifications par mail sont sécurisées par l'attribution d'un code de vérification unique et temporaire avant la saisie de mot de passe (authentification double facteur). Pour les identifiant RH, l'utilisateur doit définir un couple de « question & réponses secrètes », l'utilisateur peut choisir de renseigner un mail de recovery, et rentrera alors dans le cas de l'authentification double facteur.

La politique de mot de passe est personnalisable par le client. Par défaut, nous demandons aux utilisateurs de créer un mot de passe d'au moins 8 caractères, contenant au moins 3 parmi minuscule, majuscule, chiffre, caractère spécial. Le Client peut choisir d'activer la rotation des mots de passe, et peut définir la durée en semaine de validité d'un mot de passe.

Une solution full responsive (Tablette, smartphone, poste de travail)

Cegid Wittyfit est disponible sur l'ensemble des outils numériques du marché. Cependant pour s'assurer d'un parfait déploiement de la plateforme, il conviendra de valider les navigateurs ainsi que les devices principaux.

RGPD / CGU / gestion des identifications et traitement des données personnelles

Comme nous l'indiquions précédemment, dans le cadre de son partenariat public-privé avec le CHU de Clermont Ferrand, Cegid Wittyfit a l'obligation de se conformer, non seulement au Règlement Général de Protection des Données, mais également au Comité de Protection des Personnes du CHU.

Ainsi nous répondons à chacune des exigences que vous mentionnez en matière de sécurité, de manière non exhaustive, voici quelques-unes de nos garanties :

Hébergement de nos données chez Jaguar Network (filiale Iliad) en France métropolitaine (Marseille) avec un contrat d'hébergement HADS (logs des actions effectué sur les serveurs, cloisonnement des services, accès par habilitation)

CGU et information de l'utilisateur :

Lors de la première connexion, l'utilisateur doit lire et accepter nos CGU. Celles-ci sont claires, précises, et lisibles. En outre, pour pouvoir s'exprimer par l'intermédiaire des champs libres proposés au fil de la navigation (émission d'idées, sondage), chaque utilisateur doit lire et accepter notre "guide de bonne conduite" dans lequel est rappelé les règles de respect de la confidentialité des données de l'entreprise, et l'anonymat des personnes.

Enfin, pour davantage de protection, des messages d'information courts et précis sont proposés à chaque utilisateur sur les moyens mis en œuvre par Cegid Wittyfit afin de garantir la confidentialité des réponses et la protection des données. L'utilisateur est également informé de la finalité du traitement.

Bien évidemment, chaque utilisateur peut demander directement sur la plateforme la suppression de son compte et l'ensemble des données concernant son identifiant.

Authentification et habilitation :

Comme nous l'avons vu, les emails des collaborateurs "subissent" un chiffrement (salage et hachage via SHA512), ce chiffrement est irréversible. En outre l'identification à deux facteurs lors de la première connexion accroît encore la protection de l'utilisateur.

La date et l'heure de la dernière connexion sont présentes sur la homepage de chaque utilisateur lors de chaque nouvelle connexion, permettant à ce dernier d'en être informé s'il le souhaite.

Chiffrement :

Les données textuelles générées par les utilisateurs sont chiffrées en base (AES-512). Ce chiffrement concerne les idées émises (titre, description, commentaires), les actions (titre, description), et les champs libre des sondages.

Confidentialité

Aucune question ne comporte d'élément permettant d'identifier une personne.

Les résultats sont toujours agglomérés au sein d'équipes ou de groupes constitués de plus de **5** personnes. Cette donnée est paramétrable avec nos clients sans jamais pouvoir être inférieure à **5** répondants.

En cas d'effectifs insuffisants, non seulement le résultat du groupe ou de l'équipe ne s'affiche pas, mais celui-ci n'est même pas calculé ni stocké en base de données.

Il en est de même lors de l'analyse sur deux groupes antagonistes – Homme/Femme à titre d'exemple - Si l'effectif de l'un des deux groupes est inférieur à **5** alors l'autre groupe est également non affichable, afin d'éviter de pouvoir déduire des résultats de l'effectif total.

Dans le cadre du RGPD, Cegid Wittyfit a mis en place le poste de DPO. Sylvain AKRICHE occupe ce poste et sera votre interlocuteur privilégié : dataprivacy@cegid.com

Nous travaillons avec de grands comptes qui nous ont permis d'être certains du total respect de toutes les règles liées au RGPD. Nous vous mettrons, si vous le souhaitez, directement en lien avec nos interlocuteurs chez nos clients avec lesquels nous avons pu tester la conformité de tous nos paramètres de sécurité.

Un hébergement orienté sécurité

Nous avons confié notre hébergement à Jaguar Network (groupe Iliad). A ce titre, Cegid WITTYFIT a souscrit à son offre Agrément d'Hébergeur de Données de Santé et s'appuie sur un Système de Management Intégré (Qualité-Sécurité).

depuis 2010

depuis 2015

L'agrément HADS de Jaguar Network a été renouvelé le 2 Septembre 2019 pour une période de 3 ans.

Hébergement sécurisé de haute qualité

Techniquement, notre hébergement se constitue comme suit :

1. Services Datacenter
    - Un Datacenter Iso 27001 –equiv. Tier3, certifié HDS et PCI-DSS situé en France (Marseille) opéré par Jaguar-Network pour la partie admin-RH et pour la partie plateforme. Les 2 plateformes se trouvent sur des sous-réseaux séparés.

2. Les Datacenters sont desservis par :
    - Une connectivité haut débit et redondante,
    - Une autonomie, vis à vis des opérateurs IP grâce à la gestion d'un AS (Autonomous System)
3. Jaguar Network opère son propre réseau 40 Gbps, dont 1 Gbps dédié à la e-Santé extensible à 10 Gbps, avec support possible par son fournisseur d'accès jusqu'à 1Tbps en cas d'attaque par Deny de Service

L'infrastructure réseau

Notre infrastructure se décompose comme telle :

1. Cluster Firewalls - Junipers Networks SRX

- Des performances évolutives pour implémenter des services supplémentaires sans - aucune dégradation
- La segmentation du réseau permet aux administrateurs de créer une - sécurité et des politiques sur mesure
- Des interfaces - 10 Gb/s afin de faire face aux pics de charge
- Une protection complète contre les menaces -

2. HAProxy
   - Répartition de charge avancée (- Load Balancing)
   - Mise en place de règles de redirection spécifiques
   - Monitoring et suivi des performances -
   - Haute disponibilité (mise en cluster) -
   - Possibilité de les utiliser sans ligne internet-

Service de sauvegarde

La partie sauvegarde est orchestrée comme suit :

1. Solution de sauvegarde commvault & mylvmbackup
   - Restauration ultra-rapide des VMs, fichiers et base de données SQL
   - Prévention des pertes de données (sauvegarde rapide individuelle, en image snapshot)
   - Performance des sauvegardes optimisées
   - Vérification de la protection avec SureBackup et SureReplica
   - Rétention 7j
2. Une politique standard à 12 mois
   - Possibilité d'adapter la politique selon les besoins (suivant les obligations qui vous incombent ou s'il n'y a pas de données de santé)
3. Des sauvegardes localisées sur site distant
   - Site de production redondé à Marseille (sur 2 site)
   - Site de LYO03 (Lyon 69) pour la partie plateforme

Audit sécurité

Nous réalisons tous les ans des tests de sécurité avec Orange CyberDéfense. Sous la forme de scan de vulnérabilité, puis tests d'intrusion, nous mettons tout en œuvre pour corriger les failles selon leur criticité et nous nous engageons à fournir le rapport de contre-audit à la demande. De plus, notre hébergeur fait un suivi et corrige de manières proactive les failles remontées au fur et à mesure sur les composants le concernant.

Nos conventions de services (SLA)

Nos engagements de SLA sur le plan technique sont résumés dans le tableau suivant :

Niveau de disponibilité	
Disponibilité totale mensuelle hors indisponibilité planifiée	99.5%
Disponibilité du Service Desk	Jours ouvrés / Heures ouvrées 9h00 – 18h00
Temps d'arrêt maximum de maintenance annuelle	4H / mois maximum
Garantie de Temps d'Intervention (GTI)	2H
Garantie de Temps de Rétablissement (GTR)	24H
Astreinte	Incluse
Plage horaire d'intervention	Jours ouvrés / Heures ouvrées 9h00 – 18h00

Nos engagements de SLA sur le plan opérationnel sont résumés ci-dessous :

Une prestation de support par téléphone permettant de traiter les anomalies est disponible du lundi au vendredi inclus, de 9h à 18h. Les signalements d'anomalie doivent être confirmés par email au Prestataire sans délai. Le Prestataire procède au diagnostic de l'anomalie et met ensuite en œuvre sa correction.

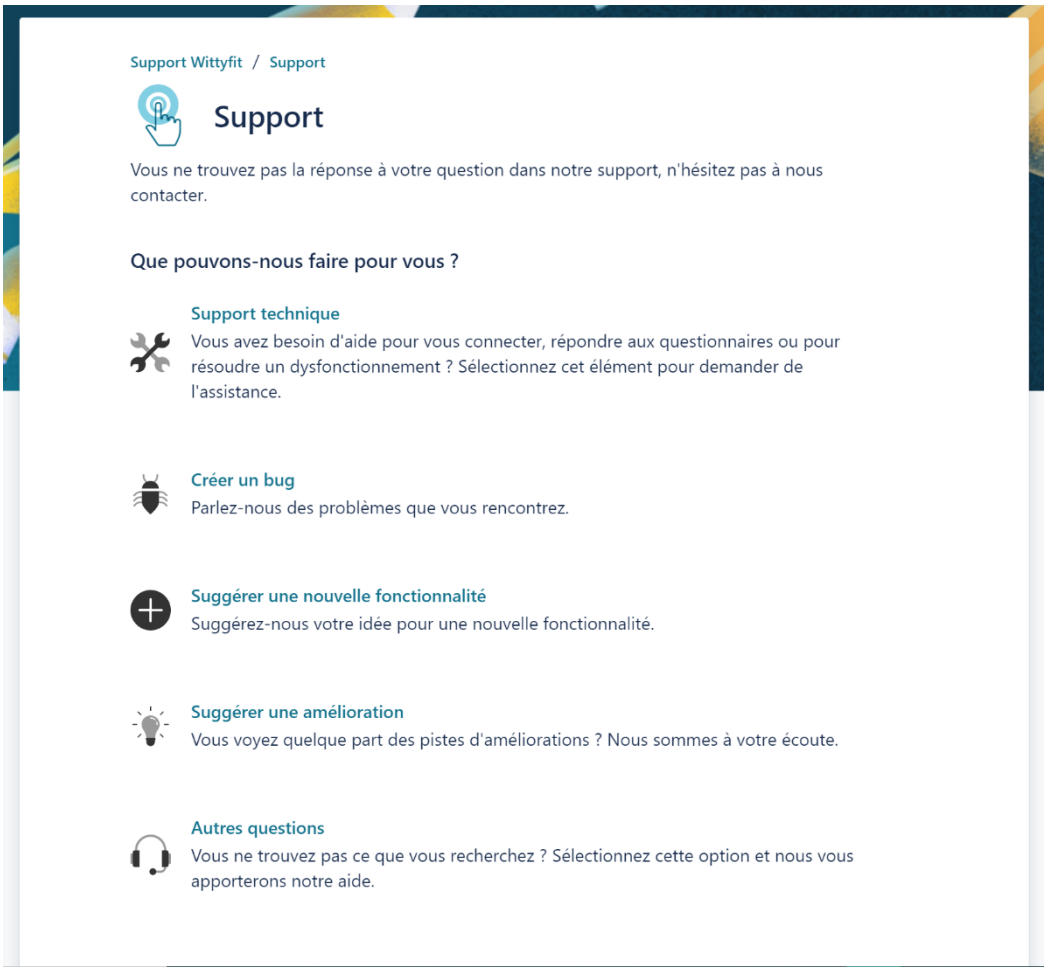
(a) En cas d'anomalie bloquante, la prise en compte du signalement intervient sous 2 heures ouvrées. Le Prestataire s'efforce de corriger l'anomalie bloquante dans les meilleurs délais, et propose une solution de contournement.

(b) En cas d'anomalie semi bloquante, la prise en compte du signalement est effectuée dans les 8 heures ouvrables.

Le Prestataire s'efforce de corriger l'anomalie, et propose une solution de contournement pouvant permettre l'utilisation des fonctionnalités en cause dans les 3 jours ouvrés.

(c) En cas d'anomalie mineure, la prise en compte du signalement est effectuée dans les meilleurs délais, et propose la correction de l'anomalie mineure dans une nouvelle version du Service applicatif qui sera livrée dans le cadre de la maintenance évolutive.

Notre plateforme on-line d'assistance permet de traiter l'ensemble des interventions suivantes :


Support Wittyfit / Support
Support
Vous ne trouvez pas la réponse à votre question dans notre support, n'hésitez pas à nous contacter.
Que pouvons-nous faire pour vous ?
Support technique
Vous avez besoin d'aide pour vous connecter, répondre aux questionnaires ou pour résoudre un dysfonctionnement ? Sélectionnez cet élément pour demander de l'assistance.
Créer un bug
Parlez-nous des problèmes que vous rencontrez.
Suggérer une nouvelle fonctionnalité
Suggérez-nous votre idée pour une nouvelle fonctionnalité.
Suggérer une amélioration
Vous voyez quelque part des pistes d'améliorations ? Nous sommes à votre écoute.
Autres questions
Vous ne trouvez pas ce que vous recherchez ? Sélectionnez cette option et nous vous apporterons notre aide.

RGPD

Préambule

Cegid Wittyfit reconnaît le caractère stratégique et strictement confidentiel de toutes les données à caractère personnel fournies par le Client. Par conséquent, Cegid Wittyfit reconnaît que l'ensemble des données et fichiers communiqués est soumis au respect de la réglementation applicable en France et dans l'Union européenne dans le domaine de la protection des données à caractère personnel (« règlementation Informatique et libertés »), incluant notamment :

- la loi relative à l'informatique, aux fichiers et aux libertés n° 78-17 du 6 janvier 1978 modifiée et ses éventuelles mises à jour ;
- la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, applicable jusqu'au 25 mai 2018 ;
- le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (règlement général sur la protection des données) abrogeant la Directive 95/46/CE, applicable à partir du 25 mai 2018 ;
- le cas échéant, les textes adoptés au sein de l'Union européenne et les lois locales susceptibles de s'appliquer aux données à caractère personnel traitées dans le cadre du Contrat ;
- les textes et décisions émanant d'autorités de contrôle, notamment de la Commission nationale de l'Informatique et des libertés (Cnil) ; et
- relève de la vie privée et du secret professionnel.

- Cegid Wittyfit est le sous-traitant du Client au sens de la l'article 28 du règlement général sur la protection des données.

- Cegid Wittyfit s'engage à mettre en place toutes les procédures nécessaires pour assurer la confidentialité et une plus grande sécurité.

Garantie

Cegid Wittyfit garantit au Client le respect des obligations légales et réglementaires lui incombant au titre notamment de la réglementation Informatique et libertés et le respect de ses obligations au titre de la présente annexe.

Le Client procèdera à toute formalité requise par la réglementation Informatique et libertés auprès d'une autorité de contrôle des données et informera, le cas échéant, les personnes concernées par le traitement de données à caractère personnel.

- Le Client est responsable du contenu et de la nature des Données Clients : il garantit notamment la licéité et la proportionnalité des données à caractère personnel contenues dans les Données Client.
- Le Client, en tant que responsable de traitement, garantit à Cegid Wittyfit que le traitement de données à caractère personnel mis en œuvre dans le cadre du Contrat satisfait aux exigences de la loi applicable et notamment que les données à caractère personnel ont été traitées de manière

licite, loyale et transparente, qu'elles ont été collectées pour des finalités déterminées, explicites et légitimes et que les informations relatives au traitement ont bien été fournies aux personnes concernées au moment de la collecte de leurs données à caractère personnel.

- Le Client doit documenter par écrit toute instruction spécifique concernant le traitement de données à caractère personnel sous-traité à Cegid Wittyfit.

Obligation du sous-traitant

Cegid Wittyfit s'engage à prendre toutes les mesures nécessaires au respect par elle-même et par son personnel de ses obligations et notamment à :

- ne pas traiter, consulter les données ou les fichiers à d'autres fins que l'exécution des prestations qu'elle effectue pour Le Client au titre des présentes ;

- ne pas traiter, consulter les données en dehors du cadre des instructions documentées et des autorisations reçues du Client, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins que Cegid Wittyfit ne soit tenue d'y procéder en vertu d'une disposition impérative résultant du droit communautaire ou du droit de l'Etat membre auquel elle est soumise, à savoir [.] ; dans ce cas, Cegid Wittyfit informera Le Client de cette obligation juridique avant le traitement des données, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;

- ne pas insérer dans les fichiers des données étrangères ;

- prendre toute mesure permettant d'empêcher toute utilisation détournée, malveillante ou frauduleuse des données et des fichiers ;

- ne pas effectuer d'étude statistique sur les données ou de traitement autre que celui demandé par Le Client sans l'approbation de ses représentants ;

- notifier dans les vingt-quatre (24) heures maximum au Client toute modification ou changement pouvant impacter le traitement des données à caractère personnel ;

- répondre dans un délai de quatorze (14) jours ouvrés à toute demande d'exercice d'un droit formulé par une personne concernée au Client ;

- informer dans les vingt-quatre (24) heures maximum Le Client si, selon elle, une instruction constitue une violation de la réglementation Informatique et libertés. Cegid Wittyfit collaborera aux travaux de réalisation de la notification à la CNIL à la demande du Client.

Par ailleurs, Cegid Wittyfit s'interdit :

- la consultation, le traitement de données autres que celles concernées par les présentes et ce, même si l'accès à ces données est techniquement possible ;

- de divulguer, sous quelque forme que ce soit, tout ou partie des données exploitées ;

- de prendre copie ou de stocker, quelles qu'en soient la forme et la finalité, tout ou partie des informations ou données contenues sur les supports ou documents qui lui ont été confiés ou recueillies par elle au cours de l'exécution du présent contrat, en dehors des cas couverts par les présentes.

- Cegid Wittyfit s'engage à prendre toute mesure utile afin de garantir que les personnes physiques agissant sous son autorité et ayant accès aux données à caractère personnel ne les traite pas, excepté sur instruction du Client, à moins d'y être obligé par une disposition impérative résultant du droit communautaire ou du droit d'un Etat membre de l'Union européenne applicable aux traitements objet des présentes. Cegid Wittyfit veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité des données ou soient soumises à une obligation légale appropriée de confidentialité.

- Elle reconnaît et accepte qu'elle ne peut agir en matière de traitement des données et des fichiers auxquels elle peut avoir accès que conformément aux présentes et au Contrat.

- En tant que sous-traitant, Cegid Wittyfit :

  - tient un registre des activités des traitements réalisés pour le compte du Client (selon les stipulations du paragraphe 5.6 ci-dessous) ;

  - communique au Client les coordonnées de son Délégué à la Protection des Données ou à défaut la personne référente en matière de protection des données de son entité.

Sécurité

- Cegid Wittyfit s'engage conformément à la règlementation Informatique et libertés, à prendre toutes précautions utiles au regard de la nature des données et des risques présentés par le ou les traitement (s), pour préserver la sécurité des données des fichiers et notamment empêcher toute déformation, altération, endommagement, destruction de manière fortuite ou illicite, perte, divulgation et/ou tout accès par des tiers non autorisés préalablement.

- Elle met en œuvre toute mesure technique et organisationnelle appropriées pour protéger les données à caractère personnel, en prenant en compte l'état des connaissances, les coûts de mise en œuvre et la nature, portée, contexte et les finalités du traitement ainsi que les risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, afin de garantir un niveau de sécurité adapté au risque.

- Cegid Wittyfit s'engage à maintenir ces moyens tout au long de l'exécution du Contrat et à défaut, à en informer immédiatement Le Client.

- Cegid Wittyfit s'engage en cas de changement des moyens visant à assurer la sécurité et la confidentialité des données et des fichiers, à les remplacer par des moyens d'une performance égale ou supérieure. Aucune évolution ne pourra conduire à une régression du niveau de sécurité.

Violations de données

- Cegid Wittyfit s'engage à notifier au Client, dans un délai de 24h après en avoir pris connaissance, toute violation de donnée à caractère personnel, soit toute violation de la sécurité entraînante, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

- Cette notification doit être envoyée à la personne désignée comme point de contact, par téléphone et/ou par courrier électronique, puis confirmée par lettre recommandée avec accusé de réception. Elle doit préciser la nature et les conséquences de la violation des données, les mesures déjà prises ou celles qui sont proposées pour y remédier et les personnes auprès desquelles des informations supplémentaires peuvent être obtenues, et lorsque cela est possible, une estimation du nombre de personnes susceptibles d'être impactées par la violation en cause.

- Lors d'une violation de données, Cegid Wittyfit s'engage à procéder à toutes investigations utiles sur les manquements aux règles de protection afin d'y remédier dès que possible et de diminuer l'impact de tels manquements sur les personnes concernées. Cegid Wittyfit s'engage à informer Le Client de ses investigations et ce de manière régulière.

- Cegid Wittyfit s'engage à collaborer activement avec Le Client pour qu'ils soient en mesure de répondre aux obligations réglementaires et contractuelles. Il revient uniquement au Client, en tant que responsable du traitement, de notifier cette violation de données à l'autorité de contrôle compétente ainsi que, le cas échéant, à la personne concernée.

Tenue du registre

- Cegid Wittyfit, en tant que sous-traitant, s'engage à tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, conformément aux dispositions du règlement général sur la protection des données. Cegid Wittyfit donnera au Client accès au registre sur demande.

Conservation des données

- Au terme du Contrat Cegid Wittyfit conservera les données de la plateforme durant 12 mois afin de permettre l'exercice des droits des utilisateurs, sauf demande explicite du Client à procéder à la destruction des données plus tôt. Au-delà de ce délai, et sauf disposition impérative contraire résultant du droit communautaire ou du droit d'un Etat membre de l'Union européenne applicable aux traitements objets des présentes, Cegid Wittyfit s'engage à détruire tous fichiers manuels ou informatisés stockant les informations collectées.

- Cegid Wittyfit s'engage à fournir au Client, à première demande, un certificat de suppression des données à caractère personnel.

Cartographie du traitement des données personnelles