Jamespot.

# Plan de conformité RGPD Jamespot (V1.1)

# Sommaire

# Introduction

En tant que sous-traitant, Jamespot a des obligations en termes de protection des données à caractères personnelles. Ce document vise à reprendre les points exposés par la CNIL et d'apporter des éléments de conformité au niveau RGPD de la plateforme.

## Liste des versions

| Version | Date | Description | Auteur(s) |
|---|---|---|---|
| V1.0 | 29/09/2020 | Création du document | Raphaël VAN-LAERE |
| V1.1 | 05/10/2020 | Ajout des mesures de sécurités | Raphaël VAN-LAERE |

## Glossaire

| Nom | Définition |
|---|---|
| RGPD | Règlement Général de la Protection des Données |
| PAS | Politique d'Assurance Sécurité |

## Sous-traitants

Afin de fournir le service, Jamespot se base sur un sous-traitant listé ci-dessous :

| Nom | Finalité | Périmètre | Référence du contrat |
|---|---|---|---|
| OVHcloud | Hébergement physique du traitement | Ensemble du traitement | 38703348 Conditions Particulières du Dedicated Cloud |
| SCALEWAY | Hébergement physique de la sauvegarde | Sauvegarde | |

## Délégué de la protection des données (DPD)

Pour toutes questions relatives au RGPD, l'adresse de contact du DPO de Jamespot est dpo@jamespot.

## Clause de sous-traitance

Une clause qui définit les obligations de chaque partie relative au données personnelles est présent dans les Conditions Générales de Service disponible sur ce lien et fourni au client lors de la signature du contrat.

# Mesures de sécurité techniques et organisationnelles

## Sécurité des serveurs

Les serveurs sont hébergés chez OVHcloud. L'hébergeur s'engage sur une sécurité optimale de ses infrastructures, notamment en ayant mis en place une politique de sécurité des systèmes d'information et en répondant aux exigences de plusieurs normes et certifications (certification PCI-DSS, certification ISO/IEC 27001, attestations SOC 1 TYPE II et SOC 2 TYPE II, etc.

La protection logique est assurée par la localisation des données de chaque client dans une Base de données distincte. Cette base est sauvegardée chaque jour et historisée dans un datacenter distinct de celui de production.

Chaque utilisateur de la solution est identifié, et dispose de droits adaptés.

L'ensemble des actions sur la plateforme est journalisé, et disponible en backoffice pour les administrateurs, avec l'horaire et l'adresse IP de l'émetteur de l'action.

Une politique de sauvegarde est mise en œuvre sur les serveurs et équipements utilisés par OVHcloud pour fournir ses services.

Tous les systèmes et données nécessaires à la continuité des services, à la reconstruction du système d'information ou à l'analyse après incident sont sauvegardés (fichiers des bases de données techniques et administratives, journaux d'activité, codes sources des applications développées en interne, configuration des serveurs, applications et équipements, etc.) ;

Les fréquences, durées de rétention et modalités de stockage des sauvegardes sont définies en adéquation avec les besoins de chaque actif sauvegardé ; la réalisation des sauvegardes fait l'objet d'un monitoring, ainsi que d'une gestion des alertes et erreurs.

## Chiffrement

La plateforme utilise le protocole HTTPS.

## Anonymisation

Effacement des données personnelles : nom, prénom, photo, qui sont remplacé par des identifiants techniques

## Cloisonnement des données

Les données restent dans ce traitement, il n'y a pas d'échange automatisés de données avec d'autre système. Chaque plateforme possède sa propre base de données, les informations sont cloisonnées et ne sont pas accessible depuis les autres plateformes.

## Contrôle des accès logiques

Jamespot a implémenté un mécanisme d'indication du degré de résistance du mot de passe. Le stockage des mots de passe est encodé et stocké en SHA256 plus SALT.

La plateforme de supervision de Jamespot permet d'accéder à tous les comptes de tous les réseaux sociaux gérés par Jamespot.

Cette fonctionnalité est utilisée à titre d'aide à l'utilisateur qui le demande, ou de reproduction de bugs dans l'environnement client.

## Traçabilité (journalisation)

Un journal des accès est disponible pour les administrateurs. Il recense l'ensemble des traces d'accès de tous les utilisateurs pendant un an.

## Contrôle d'intégrité

Le traitement intègre un processus de validation de l'entrée de donnée, essentiellement dans un but de protection des usagers. En revanche, les données étant majoritairement de type textuel, la validation de l'information n'est pas un processus automatique, de même que le dédoublonnage.

## Archivage

Les usagers peuvent décider d'archiver des ensembles d'informations en archivant un groupe. Le contenu est toujours disponible par accès dirigé, mais n'est plus proposé dans les résultats de recherche.

## Lutte contre les logiciels malveillants

Chaque système d'exploitation sur lequel est déployé la solution est maintenu à jour dans sa version pour lutter contre les failles de sécurité connues. En revanche, il n'y a pas de scan des contenus déposés par les utilisateurs dans l'immédiat. Chaque client doit s'assurer d'avoir un antivirus à jour sur le poste client pour se protéger des éventuels contenus infectés.

## Gestion des postes de travail

Chaque client doit s'assurer de la sécurité des postes de travail et des équipements mobiles permettant l'administration du service et des systèmes.

## Sécurité des sites web

Les serveurs du Datacenter peuvent être mis à jour en cas de mise à disposition de correctifs de failles critiques délivrées sur notre distribution Linux.

Les plateformes Jamespot répondent aux exigences des besoins métiers. Pour cela, les plateformes sont adaptables et intégrables avec d'autres systèmes.

On distingue donc deux profils d'utilisateurs : les administrateurs ont des droits qui surpassent les exigences de sécurité, afin de mettre en œuvre cette extensibilité.

Les droits accordés aux utilisateurs standards du système sont en revanche conformes aux recommandations de sécurité.

## Sauvegardes

Les serveurs de production sont des VMs déployées dans VSphere, suivant l'offre SDDC (Software Defined Datacenter) de OVHcloud. Les VMs sont situées sur des espaces de stockages en RAID-1 ou RAID-10, pour garantir un stockage doublé.

Les données sont sauvegardées tous les soirs, et envoyées chiffrées chez Online pour conserver une copie pendant 7 jours à un autre emplacement.

Une copie hebdomadaire stockée 1 mois, et 12 copies mensuelles stockées un an sont ensuite effectuées.

## Maintenance

Le service est normalement disponible en continue. Les évolutions sont livrées et mises en production en continue, sans période de maintenance.

## Sécurité des canaux informatiques (réseaux)

Les données sont effectivement chiffrées lorsqu'elles transitent entre les différents hébergeurs. Elles ne sont pas chiffrées à l'intérieur du réseau privé virtuel d'un même Datacenter.

## Surveillance

L'ensemble des systèmes de production est surveillé par un système de monitoring destiné à remonter des alertes, et activer les procédures de résolution d'incidents pour les incidents les plus courants.

## Contrôle d'accès physique

Ceci sont les engagements d'OVHcloud en sa qualité d'hébergeur. Les contrôles d'accès physiques sont fondés sur un système de badge. Chaque badge est lié à un compte OVHcloud, lui-même lié à un individu. Ce dispositif permet d'identifier toute personne dans les installations et d'authentifier les mécanismes de contrôle :

- Chaque individu entrant sur les sites d'OVHcloud doit avoir un badge personnel lié à son identité.
- Toute identité doit être vérifiée avant la fourniture d'un badge.
- Dans les installations, le badge doit être porté de manière visible.
- Les badges ne doivent pas mentionner le nom de son propriétaire ou le nom de l'entreprise.
- Les badges doivent permettre d'identifier immédiatement les catégories des personnes présentes (employés, tiers, accès temporaires, visiteurs).
- Le badge est désactivé dès que son propriétaire cesse d'être autorisé à accéder aux installations.
- Le badge des employés d'OVHcloud est activé pour la durée du contrat de travail. Pour les autres catégories, il est désactivé automatiquement après une période définie.
- Un badge non utilisé pendant trois semaines est automatiquement désactivé.

## Sécurité des matériels

Ceci sont les engagements pris par OVHcloud en sa qualité d'hébergeur. Des mesures de sécurité sont mises en place afin de contrôler les accès aux sites physiques d'OVHcloud :

- Une politique des droits d'accès
- Des murs (ou dispositifs équivalents) entre chaque zone
- Des caméras situées aux entrées et sorties des installations, ainsi que dans les salles de serveurs
- Des accès sécurisés, contrôlés par des badgeuses
- Des barrières laser sur les parkings
- Un système de détection de mouvement
- Des mécanismes anti-effractions aux entrées et sorties des datacenters ;
- Des mécanismes de détection d'intrusion (gardiennage 24 heures sur 24 et vidéosurveillance)
- Un centre de surveillance permanent, contrôlant les ouvertures des portes d'entrée et de sortie.

## Éloignement des sources de risque

Ceci sont les engagements pris par OVHcloud en sa qualité d'hébergeur. Des mesures sont mises en œuvre afin de prévenir les risques naturels et environnementaux.

- L'installation de paratonnerres, afin de réduire l'onde électromagnétique concomitante.
- L'aménagement des locaux d'OVHcloud dans des zones non inondables et sans risques sismiques.
- La présence d'alimentations sans interruption (UPS) de capacité suffisante et de transformateurs de secours avec basculement automatique de la charge.
- Le basculement automatique vers des groupes électrogènes disposant d'une autonomie minimale de 24 heures.

- La mise en place d'un système de refroidissement liquide des serveurs (98 % des salles d'hébergement sont dépourvues de climatiseurs).
- Le déploiement d'unités de chauffage, ventilation et climatisation (HVAC) maintenant la température et l'humidité à un niveau constant.
- La gestion d'un système de détection d'incendies (des exercices anti-incendie sont réalisés tous les 6 mois dans les datacenters).

## Organisation

Chaque Client désigne les Administrateurs de sa plateforme. Ces Administrateurs sont dès lors en contact avec le Support Jamespot. Ils seront membres des différents canaux de remontées d'information de l'équipe CSM de Jamespot, et recevrons par ces canaux les informations de sécurité générales, communes à tous les clients de Jamespot.

## Gestion du personnel

Le contrat de travail signé par les employés ainsi que la clause de confidentialité de Jamespot permettent de garantir la confidentialité nécessaire.

## Relation avec les tiers

La relation entre le Client et Jamespot est assurée par le lien entre le chef de projet Jamespot, et l'administrateur principal de la plateforme, en charge du projet chez le Client.

## Supervision

La supervision de la plateforme est assurée par le Client.

## Rétention des données

Les données sont conservées durant toute la durée du contrat. Celles-ci restent la propriété du client. Une fois le projet terminé, une copie des données sont transmis au client et sont ensuite détruite.

## Traitement hors UE

Jamespot garantie qu'aucune donnée n'est transféré hors de l'Union Européenne au sein de la plateforme.

En revanche, des composants tiers optionnels peuvent transférer des données hors Union Européenne. C'est le cas par exemple du module de tracking Google Analytics, du module ShareThis, pour partager sur les réseaux sociaux, que propose JAMESPOT, mais également les connexions SSO (Single Sign-On) avec les providers d'identité : LinkedIn, Facebook, Google. Ou encore des outils de type « Drive » : Microsoft 365, Google Workplace ou Dropbox par exemple.

## Traitement des données au sein de la plateforme

Les données présentes au sein de la plateforme sont de la responsabilité du Client.

Jamespot propose un nombre de fonctionnalité et de configuration respectant le droit en vigueur :

- La configuration par défaut des plateformes demande le strict minimum en termes de données personnelles obligatoires (adresse mail, nom et prénom).
- Lors de la première connexion, la personne doit donner son consentement pour l'utilisation des données et des cookies.
- La console RGPD permettant à tous les collaborateurs et collaboratrices de faire un export de ses données, de faire une demande de suppression ou modification de données ou encore de voir les consentements liés à son profil.

Jamespot s'engage à aider le ou la responsable du traitement des données si nécessaire.

## Documentation complémentaire

Vous pouvez trouver plus de détails dans les documents et liens suivants :

- Plan d'Assurance Sécurité
- Les CGU de Jamespot
- FAQ sécurité

# Contactez Jamespot

## Jamespot - Siège social

66 rue Marceau (Bâtiment C')

93100, Montreuil

+33 (0)1 48 58 18 01

info@jamespot.com

## Jamespot - Pôle Ouest

2 Rue de la Mabilais

35000, Rennes