

FICHE DE REGISTRE DE L'ACTIVITÉ PLANZONE

Date de création de la fiche	Mercredi 8 Novembre
Date de dernière mise à jour de la fiche	Mercredi 8 Novembre
Nom du responsable conjoint du traitement (dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)	DPO – Laurent Raynaud
Nom du logiciel ou de l'application (si pertinent)	Planzone

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.

Suivi de l'utilisation des utilisateurs de Planzone.

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données.

Exemples : salariés, usagers, clients, prospects, bénéficiaires, etc.

1. Usagers du logiciel Planzone

Catégories de données collectées

Cochez et listez les différentes données traitées

☒ État-civil, identité, données d'identification, images (ex. nom, prénom, adresse, photographie, date et lieu de naissance, etc.)

Nom
Prénom
E-mail
Pays
Langue principale

☐ Vie personnelle (ex. habitudes de vie, situation familiale, etc.)

Aucune

☒ Vie professionnelle (ex. CV, situation professionnelle, scolarité, formation, distinctions, diplômes, etc.)

Société
Poste
N° de tel professionnel

☐ Informations d'ordre économique et financier (ex. revenus, situation financière, données bancaires, etc.)

Aucune

☒ Données de connexion (ex. adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)

- Adresses IP
- Informations de connexion à l'application :
 - o Date de création du compte
 - o Date du dernier accès

☐ Données de localisation (ex. déplacements, données GPS, GSM, ...)

Aucune

☒ Internet (ex. cookies, traceurs, données de navigation, mesures d'audience, ...)

Uniquement les cookies de session de l'application.

☐ Autres catégories de données (précisez) :

Aucune

Des données sensibles sont-elles traitées ?

La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).

☒ Non

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

19 mois (dont 1 pour la suppression de la sauvegarde) à compter de la fin de la relation contractuelle puis supprimées ou sont immédiatement supprimées si demandé par le souscripteur.

Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre.

Catégories de destinataires des données

Destinataires internes

Aucun destinataire externe

Organismes externes

Aucun organisme de traitement externe

Sous-traitants

Aucun Sous-Traitant

Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'Union européenne ?

☒ Non

Mesures de sécurité

Cochez et décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données.

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.

☒ Contrôle d'accès des utilisateurs

Décrivez les mesures :

L'accès aux outils et interfaces d'administration est limité aux seules personnes habilitées

☒ Mesures de traçabilité

Précisez la nature des traces (*exemple : journalisation des accès des utilisateurs*), les données enregistrées (*exemple : identifiant, date et heure de connexion, etc.*) et leur durée de conservation :

Logs de connexion pseudonymisés incluant :

- Id de l'utilisateur
- La date et heure de l'action
- Id de la Planzone
- Nature de l'action

Ceux-ci sont conservés jusqu'à 19 mois après résiliation du souscripteur puis supprimées ou immédiatement supprimées après résiliation si le souscripteur en formule la demande.

☒ Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Décrivez les mesures :

Technologie SSL pour les échanges de données entre le client et le serveur Planzone.

Réseaux virtuels privés (VPN)

Pare-feu

Mécanisme côté applicatif

☒ Sauvegarde des données

Décrivez les modalités :

Sauvegarde journalière conservée 1 mois.

☒ Chiffrement des données

Décrivez les mesures (*exemple : site accessible en https, utilisation de TLS, etc.*) :

SSL, SHA-1 pour les mots de passe SHA-256 avec chiffrement RSA (1.2.840.113549.1.1.11) pour les échanges de données dans l'application

☐ Contrôle des sous-traitants

Décrivez les modalités :

Pas de mesures liées aux sous-traitants car nous ne travaillons avec aucun sous-traitant concernant le traitement des données.

☒ Autres mesures:

Présence d'une politique de gestion et de création des mots de passe sur l'application/outil visé ?	Nous utilisons OWASP comme protocole de sécurité lié à la gestion et la création des mots de passe
Garanties concernant la proportionnalité des données traitées ?	Nous appliquons le concept privacy by design pour garantir la proportionnalité des données traitées
Garanties concernant la minimisation des données traitées ?	Les seules données collectées des utilisateurs sur Planzone sont en rapport avec leur fonction, leur statut et leur nom dans un but de gestion des ressources et le paramétrage du profil personnel.
Garanties concernant la mise en œuvre du principe de sécurité des données par défaut ?	Le principe de sécurité par défaut a été approuvé dès 2010 lors de la release publique de Planzone. De multiples audits ont été réalisés pour évaluer la sécurité de l'applicatif avant sa release.
Garanties concernant la confidentialité des données traitées ?	Nos informations ne sont communiquées à aucun tiers https://www.planzone.fr/infos/confidentialite
Définition des modalités de mise en œuvre de la réversibilité des données ?	A l'issue du contrat, vous pourrez récupérer vos données sous la forme d'une archive CSV, SQL ou JSON.
Présence d'une procédure d'effacement des données ?	Tout client peut s'il le souhaite, réclamer la suppression totale des données le concernant.



Politique de sécurité de Planzone 7
Version 3.1 du 9 juillet 2024

Contents

1	Fiche de suivi	2
1.1	Modifications	3
1.2	Diffusion	3
2	Introduction	3
2.1	Glossaire :	3
3	Politique RH et sécurité	4
4	Sécurité physique	4
5	Gestion des accès	4
5.1	Accès aux infrastructures informatiques	4
5.2	Accès à notre application Saas	5
5.3	Accès aux applications de développement	5
6	Accès aux données	5
7	Développement	6
8	Gestion des changements	7
9	Gestion des vulnérabilités	7
10	Suivis et rapports	8
11	Gestion des incidents	8
12	Continuité de l'activité	8
13	Conformité	9
14	Protection des informations en cours de transfert	9
15	Sécurité de la plateforme serveur	9
16	Disponibilité	10
17	Confidentialité	10
18	Intégrité	10
19	Conclusion	10

1 Fiche de suivi

Statut	Validation en cours
Classification	Public
Auteur	Arnaud Lapr�vot� (arnaud.laprevote@planzone.com)
Date	21/05/2024
Approuv� par	
Date	
Version	plz7sec-01.00.03

1.1 Modifications

Date	Objet	Auteur
12/05/2024	Cr�ation	Arnaud Lapr�vot�
08/07/2024	Mise � jour (pen testing, clarifications, page de titre)	Arnaud Lapr�vot�

1.2 Diffusion

Nom	Adresse mail	Pour _I_nfo/_A_ction
Arnaud Lapr�vot�	arnaud.laprevote@planzone.com	A
Virna Ing	virna.ing@augeo.com	A
Maroua Jellal	maroua.jellal@augeo.com	I
Adel Bensalem	adel.bensalem@augeo.com	I
Elie Iniesta	elie.iniesta@augeo.com	A
Laurent Raynaud	laurent.raynaud@augeo.com	A
R�mi Aldeguer	remi.aldeguer@augeo.com	I

2 Introduction

Augeo Software, propri taire des Services Planzone, a con u cette politique s curit  afin de d montrer notre fort engagement concernant la s curit  pour notre logiciel Planzone.

2.1 Glossaire :

Terme	D�finition
planzone	L'espace de travail d'une organisation dans laquelle elle peut d�finir des zones, des portefeuilles de projets, des ressources, des projets et les �l�ments associ�s (liste de t�ches, t�ches, �v�nements, jalons, affectation d'une ressource � une t�che, un �v�nement ou un jalon, temps pass� sur une t�che).
zone	Un regroupement arbitraire de projets dans la planzone
portefeuille	Des projets d�finis dans des zones peuvent �galement �tre regroup�s en "portefeuilles", et ce ind�pendamment de leur zone
projet	Un ensemble de liste de t�ches, de t�ches, de jalons et d'�v�nements regroup�s. Des ressources (mat�rielles, humaines et virtuelles) sont associ�es � un projet. Ces ressources peuvent aussi �tre associ�es � une t�che, un jalon ou un �v�nement. On parle alors d'allocation.

3 Politique RH et sécurité

- Nous n'effectuons pas de vérification des antécédents de tout le personnel concerné. Cependant, l'équipe de développement de l'entreprise compte moins de 10 personnes, qui sont individuellement connues, avec un faible turnover et dont les parcours sont connus et vérifiés à l'embauche. Nous sommes donc confiant dans notre personnel.
- L'accord de confidentialité entre les personnes travaillant pour Augeo est inclus dans leur contrat de travail. Lors de l'emploi de contractuels, ces derniers n'ont jamais accès directement au code mis en production, une revue de code est systématiquement faite par des salariés d'Augeo. L'exploitation est confiée à des salariés d'Augeo. Nous avons un prestataire qui nous assiste dans les tâches liées à l'exploitation des serveurs. Nous travaillons avec ce prestataire français depuis 5 ans. Le contrat nous liant inclus des règles de confidentialité.
- Nous faisons une conférence de sensibilisation à la cybersécurité tous les 3 mois avec les différents salariés de l'entreprise.
- Tous nos utilisateurs ont une bonne compréhension de la sécurité et les administrateurs et développeurs n'ont pas besoin de formation supplémentaire.
- Une procédure formelle dictant les actions à entreprendre lorsqu'un utilisateur a violé des politiques de sécurité de l'information est défini dans la procédure de gestion des ressources humaines de notre entreprise.

4 Sécurité physique

- Planzone 7 est une application Saas. Nous fournissons les infrastructures (via notre partenaire OVH) hébergées en France et accueillant vos données.
- Le bâtiment où nous travaillons est sécurisé en dehors des bureaux (immeuble fermé, gardiennage, bureau fermé, clé de sécurité). Nous nous reposons sur l'excellente politique de sécurité physique d'OVH pour les accès physiques à nos serveurs.
- OVH notre fournisseur de cloud est certifié ISO 27001.
- La sécurité extérieure de l'entreprise comprend des portes et des barrières, et un bureau de sécurité humaine.
- Les utilisateurs doivent verrouiller leur poste lorsqu'ils s'absentent.

5 Gestion des accès

5.1 Accès aux infrastructures informatiques

- Le personnel administratif, commercial et la direction générale de l'entreprise n'ont pas d'accès d'administration aux infrastructures de fourniture du service de l'entreprise. Seuls les personnels ayant à en connaître et pouvant être amenés à exploiter, déployer, déboguer ont un accès sécurisé à ces infrastructures.
- Les documentations des systèmes que nous exploitons (hors information de connexion) sont disponibles pour tous les personnels de l'entreprise.
- Notre personnel informatique sait que lorsque l'informatique est délivré aux nouveaux membres, ils ne doivent donner accès qu'aux ressources dont ils ont réellement besoin.
- Les personnels externes ont des accès aux infrastructures de développement et de test, mais pas aux infrastructures de production ou pré-production.
- L'accès aux infrastructures d'exploitation (test, développement, pré-production, production) se fait via un serveur bastion et via ssh uniquement avec des clés cryptographiques protégées.
- Moins de 10 utilisateurs ont accès au serveur bastion.
- Nous faisons une revue des accès et des droits sur nos applications au moins tous les 3 mois.

- Nous utilisons le service de base de données d'OVH comme base de données. Nous exploitons le service S3 fourni par OVH pour le stockage des fichiers.
- L'accès aux données des clients en production est limité à une équipe de salariés permanents d'Augéo auquel s'ajoute un prestataire externe avec lequel nous travaillons au moins depuis 5 ans.
- Les mots de passe des clients sont stockés en utilisant l'algorithme bcrypt.
- Un accès par API est disponible pour l'application. Le trafic est chiffré par TLS.
- Nos environnements hors production doivent avoir des contrôles réduits en raison de notre méthodologie de développement.

5.2 Accès à notre application Saas

- Les utilisateurs de nos applications utilisent un login/mot de passe pour l'accès aux applications fournies par l'entreprise.
- Nous faisons une revue des accès et des droits sur nos applications au moins tous les 3 mois.
- Lors de votre enregistrement ou lorsque vous êtes invité à rejoindre un Espace de Travail collaboratif Planzone, nous vous demandons de choisir et d'entrer un mot de passe. Votre mot de passe est chiffré avec l'algorithme Bcrypt et enregistré en format crypté. Votre mot de passe ne vous sera jamais transmis par quelque moyen que ce soit. Il n'est pas accessible aux collaborateurs d'Augéo.
- Si vous avez oublié votre mot de passe, ou que votre mot de passe ne fonctionne pas pour quelque raison que ce soit, une procédure de changement de mot de passe est mise à votre disposition.

5.3 Accès aux applications de développement

- Pour la gestion des comptes utilisateurs des applications internes, nous exploitons les fonctionnalités de Google Workspace afin de centraliser l'accès aux données de l'entreprise. Nous l'utilisons aussi pour l'authentification sur des services tiers (par exemple gitlab.com). Nous nous appuyons sur les politiques de sécurité de Google pour la bonne gestion des identités.

6 Accès aux données

- Les Services Planzone s'appuient sur un ensemble de solutions et procédés techniques nécessaires pour assurer la sécurité des données et l'échange sécurisé des informations professionnelles entre Utilisateurs.
- Seuls les membres d'un Espace de Travail collaboratif (dit Planzone, cf glossaire) peuvent visualiser et accéder aux contenus de cet espace. En fonction des droits d'accès aux données définis par le titulaire du compte Planzone ou par un utilisateur désigné par ce dernier, un utilisateur peut ne pas voir certaines données de l'Espace de Travail ou ne pas être capable d'actualiser certaines informations. Les paragraphes suivants détaillent ces droits.
- Un système de droit est mis en oeuvre dans Planzone 7. Ce système de droit est organisé avec des niveaux d'accès et de modification aux informations. Au niveau global d'une Planzone, 4 niveaux de droits sont définis : administrateur, sous-administrateur, utilisateur, visiteur. Un administrateur a le droit d'accéder et de modifier toutes les informations d'une planzone. Le sous-administrateur peut créer des projets de manière généralisée dans les différentes zones. Cependant, il ne peut accéder de manière générale aux informations d'autres zones et projets (sur lesquels il n'est pas acteur). L'utilisateur ne peut pas créer de zones, de projets ou de

ressources sur la Planzone. Il ne peut qu'accéder aux zones et aux projets auxquels il est associé. Finalement, le visiteur ne peut que voir les projets où il est associé.

- En ce qui concerne les projets sur la plateforme, un utilisateur peut avoir 3 rôles différents : il peut être “chef de projet”, “collaborateur” ou “observateur”. Le chef de projet peut modifier tous les éléments du projet et inviter des utilisateurs enregistrés ou inviter des utilisateurs à participer au projet. Le collaborateur peut créer et modifier les tâches, les événements, les jalons et les listes d'un projet. Il ne peut pas inviter ou ajouter de ressources sur le projet. Finalement, un observateur peut voir les éléments du projet, mais ne peut pas les modifier à l'exception des commentaires qu'il peut ajouter. L'observateur peut remplir sa feuille de temps, mais ne peut pas voir la synthèse des temps passés pour les projets.
- Au niveau de la programmation, un système de très bas niveau (Row Level Security) assure qu'un utilisateur ne peut voir que les informations auxquelles il a le droit d'accéder.

7 Développement

- Nous utilisons un système de contrôle de version de code reconnu (Git) pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes que nous développons et maintenons.
- Nous utilisons Jira pour gérer le travail, les exigences et les problèmes.
- Nous utilisons Confluence ou un système similaire pour développer et collaborer sur la documentation.
- Nous utilisons un outil d'intégration / de déploiement continu (CI / CD) de cycle de vie complet (GitLab) pour prendre en charge nos systèmes depuis le développement et jusqu'à l'exploitation.
- Nous utilisons un outil de gestion de projet pour gérer les tâches et prévoir la livraison.
- Il nous arrive d'utiliser des données d'organisation utilisatrice pour les tests lors du développement. Dans ce cas, nous obtenons l'autorisation formelle de cette organisation pour le faire. Nous favorisons des organisations publiques dont nous savons que les données sont non confidentielles.
- Nos systèmes de test et de développement sont identiques en matière de sécurité avec nos environnements de production. Nous avons simplement plus de personnes autorisées à y accéder.
- Nous minimisons les bibliothèques que nous utilisons. Dans le cas de l'environnement de back-end, nous utilisons un environnement springboot fourni et maintenu par une société tierce qui assure la surveillance des failles de sécurité.
- Nous avons une équipe de test interne qui vérifie chaque version pendant le développement et avant la publication.
- Chaque module applicatif (authentification, gestion des utilisateurs, coeur fonctionnel, application web) a un responsable qui regarde et valide les modifications avant l'intégration dans le code qui est mis en test.
- Les droits associés aux différents rôles sont définis lors de la spécification des différents micro-services. Une couche “profonde” du back-end gère la sécurité (utilisation du Row Level Security).
- Les développeurs sont conscients de l'importance de la sécurité dans le développement applicatif.
- L'application est basée sur un ensemble de micro-services qui exploitent les informations d'authentification pour connaître les droits d'un utilisateur faisant une demande.
- Notre développement utilise la méthodologie Agile (daily, sprint review, sprint planning, ..., scrum master, product owner).
- Nous appliquons des tests de système complet avant tout déploiement en production (versions majeures et mineures).
- Nos développeurs décident quels composants tiers sont requis et ils sont chargés de vérifier leur fiabilité. Dans le cas du front-end en javascript nous avons une trentaine de dépendances, dont

10 liées à react. Etant donné la taille de l'application, c'est un nombre très limité de dépendance. Dans le cas du back-end, nous utilisons une distribution de springboot maintenue par une société tierce qui assure aussi le suivi de sécurité.

- Nous procédons à un pentesting de planzone7 une fois tous les 12 à 18 mois par une entreprise tierce spécialisée. Le dernier pen testing a eu lieu en juin 2024. Des actions correctives ont été prises suite à ce test.
- Nous effectuons des révisions de code statique pour éviter les codes troyens.
- Tous nos développeurs comprennent l'importance du codage sécurisé. Nous exploitons une couche de sécurité de bas niveau dans notre back-end pour éviter des accès indésirés aux données. (Row level Security).
- Nos techniques de validation des entrées et des sorties sont les suivantes :
 - Le code client / navigateur valide que toutes les valeurs d'entrée sont du type et du format corrects
 - Le code côté serveur valide que toutes les valeurs d'entrée sont du type et du format corrects
 - Le code côté client / navigateur vérifie que les valeurs d'entrée sont comprises dans les plages autorisées
 - Le code côté serveur vérifie que les valeurs d'entrée sont comprises dans les plages autorisées
 - Toutes les interactions avec les bases de données sont d'abord transmises via un code côté service conçu spécifiquement pour supprimer les risques d'injection SQL.
 - Aucune donnée de sortie n'a une route directe de la base de données vers l'interface utilisateur
- Mesures de sécurité utilisées dans notre environnement de production :
 - Tous nos serveurs d'application et micro-serveurs ont des pare-feux intégrés avec un accès limité aux communications requises
 - Nos bases de données ont les historiques d'accès et de transactions activés
 - Les historiques système sont activés
- Protection pour notre application en environnement de production :
 - Nous avons des pare-feux de niveaux 3/4 en place avec des règles limitant les connexions aux seuls ports et protocoles requis pour le fonctionnement
 - Nous utilisons des proxys inversés pour empêcher nos serveurs d'applications d'être exposés à des attaques malveillantes

8 Gestion des changements

- Les changements sont mis en oeuvre par l'équipe de développement sur demande
- Aucun matériel informatique au sein de notre entreprise ne stocke les données des clients.
- Nous enregistrons les modifications de notre système d'information utilisé pour héberger Planzone 7.
- Les modifications sont construites et testées dans un environnement de test représentatif, distinct des environnements de développement et de production, avant d'être déployées en production avec l'approbation du directeur technique et des développeurs leads.
- Nous essayons de minimiser les temps d'arrêt du système, mais parfois nous devons mettre les systèmes hors service pour mettre en oeuvre le changement

9 Gestion des vulnérabilités

- Toutes les vulnérabilités identifiées sont conservées dans un registre et nos administrateurs tentent de les corriger le plus rapidement possible

- Les clients sont autorisés à faire une évaluation des vulnérabilités externes après consultation et en collaboration avec notre équipe informatique
- La gestion des correctifs tente d'appliquer rapidement des correctifs de haute priorité ou d'urgence (par exemple dans les 30 jours), mais ce n'est pas toujours possible en raison de l'impact que les changements peuvent avoir sur nos systèmes.

10 Suivis et rapports

- Nous travaillons à une refonte de notre système de monitoring pour notre infrastructure de production
- Nous stockons les connexions des utilisateurs à notre système mais ensuite nous ne stockons pas ni n'analysons l'utilisation de notre système
- Nous enregistrons les tentatives de connexion infructueuses
- Nous stockons tous les historiques au moins 30 jours

11 Gestion des incidents

- Nos processus de gestion des incidents sont bien définis et la gestion de la configuration est conduite de manière réactive en fonction des circonstances de l'époque
- Nous n'avons pas d'équipe d'intervention dédiée à la sécurité de l'information et aucun moyen de collecte de preuves
- Les rapports d'incident ne sont pas transmis à la direction. Elle est informée oralement de ce type de problèmes.
- Nous ne faisons pas d'examen systématiques des procédures et politiques après un incident, même si ces dernières évoluent régulièrement.
- Notre SLA n'inclut pas de paramètres d'enquête en standard.

12 Continuité de l'activité

- Nos plateformes sont basées à 100% sur le cloud, sans données stockées sur site, à l'exception de la mise en cache locale. Notre fournisseur de cloud a adopté des mesures de protection de l'environnement conformes aux bonnes pratiques reconnues de l'industrie.
- Notre fournisseur de cloud utilisent des systèmes d'extinction d'incendie installés dans les centres de données (pré-action, brouillard, humide, agent propre, etc.). Cette responsabilité incombe à notre fournisseur de cloud et s'appuie sur au moins un niveau de géo-redondance
- Le risque de catastrophe naturel est au plus bas : tous les systèmes sont basés sur le cloud pour permettre une utilisation à partir d'autres environnement de bureau ou de travail à domicile.
- Les procédures de sauvegarde sont documentées et surveillées pour s'assurer qu'elles sont correctement suivies.
- La sauvegarde est exclusivement faite en stockage cloud.
- Un coordinateur de plan de reprise après sinistre n'a pas été nommé.
- Un scénario du "pire cas" est en cours de rédaction avant d'être testé.
- Une liste des numéros de téléphone d'urgence actuelle de la police, des pompiers, de l'aide médicale et des responsables de l'entreprise a été stratégiquement localisée au siège.
- Le site de sauvegarde est situé à plus de 100 km du site principal.
- Un PRA doit être mis en place dans les 9 mois.
- Notre engagement de pourcentage de disponibilité est supérieur à 99%.
- Nous assurons la disponibilité car notre logiciel SaaS s'appuie sur un cloud haute disponibilité.
- Nous disposons de plusieurs connexion internet au site de l'entreprise.

- En cas de sinistre, notre environnement de pré-production est sur des serveurs différents de notre environnement de production. Il est possible de basculer sur ce serveur en attendant un serveur de production.
- Nous ne nous engageons pas dans notre garantie de niveau de service dans les conditions de reprise après sinistre

13 Conformité

- Les politiques et procédures de sécurité sont régulièrement testées par notre équipe informatique
- Les exceptions aux politiques et procédures de sécurité doivent être approuvées par le directeur technique au minimum par mail
- Lorsqu'un employé ne respecte pas les politiques de sécurité, des mesures disciplinaires appropriées sont prises, elles sont cependant informelles et non enregistrées
- Des audits ad hoc sont menés régulièrement entre tous les 12 à 18 mois
- Nous n'effectuons pas d'audit surprise
- Il n'y a pas de responsable de la gestion des résultats d'audit.
- Nous pouvons fournir les historiques de connexion à l'auditeur.

14 Protection des informations en cours de transfert

Les Services Planzone utilisent un moyen de cryptologie intégré dans votre navigateur pour garantir le transfert sécurisé de vos informations et documents lorsque vous avez ouvert une session sur Planzone. Nous utilisons un cryptage Secure Socket Layer (SSL) avec une longueur de clé de chiffrement jusqu'à 128 bits pour l'échange de données entre votre navigateur et nos serveurs.

15 Sécurité de la plateforme serveur

Nous avons adopté des moyens adaptés de collecte, de stockage et de traitement de données, ainsi que des mesures de sécurité logicielle et physique spécifiques pour nous protéger contre l'accès, la modification, la divulgation ou la destruction non autorisées de vos informations personnelles et autres données de votre compte. Tous nos serveurs sont hébergés dans un DataCenter français d'OVH, leader européen sur le marché de l'hébergement informatique. De strictes procédures de sauvegarde et de sécurité sont appliquées régulièrement sur nos machines.

OVH répond aux normes ISO 27001, ISO 27017, ISO 27018, SOC 1 (anciennement SAS 70), SOC 2 et SOC 3 Security & Availability, PCI DSS Niveau 1, Hébergeur de Données de Santé (HDS) et bien d'autres (<https://www.ovhcloud.com/fr/entreprise/certification-conformity/>).

Nous considérons que nous ne pouvons pas être responsable de la sécurité au niveau de l'ordinateur de l'utilisateur final. Si un attaquant prend pied sur ce poste, il pourra accéder aux informations auxquels un utilisateur a accès.

Par contre, nous sommes particulièrement précautionneux concernant la sécurité des serveurs que nous utilisons. Plusieurs mesures sont en oeuvre pour cette sécurisation :

- utilisation d'un bastion pour les accès d'administration,
- revue mensuelle des droits d'accès sur ce bastion et sur les autres systèmes impliqués,

Nous travaillons de manière continue sur l'amélioration de la sécurité des différents éléments.

16 Disponibilité

Une architecture redondante nous permet de vous assurer que, même en cas de dysfonctionnement d'un serveur de production, un autre serveur prendra le relais et vous donnera accès à vos informations sans interrompre votre travail d'équipe. Nous proposons aujourd'hui à nos clients de garder un accès à leurs données 24/7, de partout dans le monde.

17 Confidentialité

Une plateforme collaborative vise bien évidemment à faciliter l'échange des données de vos projets. Cela ne signifie pas toutefois qu'il faut rendre ces données accessibles à des personnes extérieures, ou rendre publiques par erreur des informations qui n'y sont pas destinées. Comme vous pouvez le constater en consultant notre Charte de confidentialité, nous sommes particulièrement engagés pour le respect des règles de confidentialité.

Les données de vos projets peuvent être consultées uniquement par un membre de votre espace de travail (un membre de votre Planzone). Seuls les personnels d'administration de Planzone ont accès à vos données.

18 Intégrité

De nombreuses entreprises du Fortune500 font déjà confiance à la fiabilité de nos centres d'hébergement de données. Nous faisons appel aux dernières technologies de pointe pour sécuriser les données stockées sur les serveurs, et une partie de notre équipe travaille à temps complet sur l'amélioration des procédés employés pour la sécurisation des données.

Tous les changements effectués sur les données sont enregistrés et suivis. Les données de nos serveurs sont sauvegardées quotidiennement.

19 Conclusion

Le responsable de la politique de sécurité est Arnaud Laprevote joignable par mail à arnaud.laprevote@planzone.com.