

Mesures techniques et organisationnelles de sécurité

Définitions

« Donnée personnelle » : se définit comme « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres », conformément à la loi Informatique et libertés du 6 janvier 1978.

« Client » : désigne une personne morale ou physique souscrivant à l'une des offres proposées par le prestataire de services pour la solution « hoopop ».

« Service » désigne la société « chroma.team » mettant à disposition la solution « hoopop » pour le Client tels que prévus dans le Contrat Principal incluant des Traitements de Données Personnelles objets du présent Avenant.

Introduction

Ce document décrit les mesures techniques et organisationnelles de sécurité mis en place par le Service pour protéger les données personnelles et assurer la confidentialité, l'intégrité et la disponibilité continues de nos produits et services.

Les informations explicités ci-dessous sont un aperçu général des solutions techniques et organisationnelles mis en place par le Service. Si nécessaire, il est possible d'obtenir des détails supplémentaires, sur demande, à l'adresse e-mail suivante : rgpd@hoopop.app.

Le Service se réserve le droit de réviser ces mesures techniques et organisationnelles à tout moment, sans préavis, dès lors que celles-ci ne dégradent pas le niveau de protection des données personnelles actuel.

Dans le cas, peu probable, d'un accès non autorisé aux données personnelles, le Service en informera le Client dans des délais cohérents et à la suite des changements et à la mise en place des ajustements techniques et organisationnels nécessaires.

Mesures

Le Service met en place les mesures techniques et organisationnelles de sécurité suivantes afin de protéger les données (personnelles et non personnelles) :

L'ordre de ces mesures ne représente aucun classement particulier ou tout autre tri par ordre d'importance.

- Une équipe dédiée est chargée de la mise en œuvre et de la maintenance des politiques et des mesures de sécurité de l'information du Service.
- Les serveurs et systèmes du Service utilisent des journaux d'événements et des techniques d'audit associées pour enregistrer l'accès des utilisateurs et l'activité du système en vue d'un examen périodique.

- L'accès par voie électronique aux données (personnelles et non personnelles) via les serveurs et systèmes du Service est strictement soumis à des contrôles d'accès selon des niveaux d'autorisations clairement définis et pour un ensemble connu et restreint d'utilisateurs.
- Les identifiants et mots de passe d'accès, par voie électronique, aux données (personnelles et non personnelles) via les serveurs et systèmes du Service sont soumis à une politique stricte de rotation régulière des mots de passe, uniques, forts et complexes ainsi qu'à l'utilisation obligatoire d'une double authentification 2FA.
- Des procédures de résilience des activités et de reprise, sont mises en place pour maintenir le Service après des situations d'urgence ou des sinistres prévisibles et imprévisibles.
- La sécurité physique et environnementale des centres de données du Service est assurée par la politique de sécurité associée et fournie par nos hébergeurs.
- Des protocoles cryptographiques standards et conformes aux normes industrielles sont utilisés pour le stockage et le transfert des données (personnelles et non personnelles) entre les applications, les serveurs et les systèmes du Service.

Hébergement des données

L'ensemble des données (personnelles et non personnelles) du Service sont réparties et hébergés chez deux (2) fournisseurs et centres de données : *Amazon Web Services (AWS)* et *Wasabi Technologies (Wasabi)*

Amazon Web Services (AWS)

Où ?

Des données (personnelles et non personnelles) du Service sont hébergés en Irlande, plus précisément à Dublin dans la région « eu-west-1 » comme nommée par *Amazon Web Services (AWS)*.

Plus d'informations sur la localisation de *Amazon Web Services (AWS)* : https://aws.amazon.com/fr/about-aws/global-infrastructure/regions_az/

Comment ?

Des données (personnelles et non personnelles) du Service sont sauvegardées dans des bases de données répliqués et hautement disponibles en utilisant un chiffrement avancé des données, qu'elles soient en transit ou au repos.

Quelles données ?

L'ensemble des données textuelles (personnelles et non personnelles) saisies, par le Client, dans les champs et formulaires des différentes applications du Service.

Wasabi Technologies (Wasabi)

Où ?

Des données (personnelles et non personnelles) du Service sont hébergées aux Pays-Bas, plus précisément à Amsterdam dans la région « eu-central-1 » comme nommée par *Wasabi Technologies (Wasabi)*.

Plus d'informations sur la localisation de *Wasabi Technologies (Wasabi)* : <https://wasabi.com/fr/sites/>

Comment ?

Des données (personnelles et non personnelles) du Service sont sauvegardées dans systèmes de stockage de fichiers répliqués et hautement disponibles en utilisant un chiffrement avancé des données, qu'elles soient en transit ou au repos.

Quelles données ?

L'ensemble des fichiers et images contenant des données (personnelles et non personnelles) envoyées, par le Client, dans les champs dédiées des différentes applications du Service.

Schéma de l'hébergement

