

*Cette traduction est fournie à titre informatif uniquement. La version anglaise de cette page fait foi.*

# Aperçu de la sécurité et de la protection de la vie privée

Chez FareHarbor, notre mission est de vous aider à gérer et à développer votre activité grâce aux meilleurs outils de réservation et de logistique disponibles. Nous considérons la sécurité et la protection de la vie privée comme l'une de nos responsabilités les plus importantes dans la réalisation de cette mission. Chaque section ci-dessous développe une approche qui vise à satisfaire ou dépasser les exigences de conformité qui s'appliquent aux données et à la sécurité de votre entreprise.

## **RGPD**

Le Règlement général sur la protection des données (RGPD) est la norme de confidentialité des données dans l'Union européenne (UE) qui régit la protection des données personnelles de ses résidents. Pour vous aider à vous conformer au RGPD, nous mettons à votre disposition les aides suivantes :

### **Le droit d'être informé.**

Veuillez noter qu'en tant que prestataire d'activités, vous agissez en tant que responsable du traitement des données de vos clients et à ce titre, vous êtes légalement tenu(e) de leur fournir des informations sur les données personnelles les concernant qui sont collectées, utilisées, consultées ou traitées d'une autre manière, et sur la mesure dans laquelle vous traitez ou traiterez ces données personnelles. Dans le cadre du RGPD, le terme « traité » a une définition très large qui comprend, entre autres, la collecte, l'enregistrement, la structuration, le stockage, l'adaptation, l'utilisation, l'effacement ou la destruction des données personnelles. À votre demande, nous mettrons à votre disposition les informations que vous avez demandées si nous sommes les seuls à pouvoir fournir ces informations et si cela est nécessaire pour vous conformer aux obligations du RGPD.

### **Accès aux données, portabilité, rectification et effacement.**

Après avoir effectué une réservation, vos clients peuvent demander à ce que leurs données stockées leur soient communiquées et, si besoin, supprimées. En soumettant un formulaire par l'intermédiaire de FareHarbor.com, vous pouvez également demander que vos données stockées soient fournies et, le cas échéant, supprimées. Les

demandes concernant les données peuvent être effectuées via notre [Formulaire de demande relative aux données](#).

Toutes les demandes relatives aux données sont examinées et authentifiées par un système de sécurité. Les données des demandes authentifiées sont supprimées dans un délai de 30 jours. Une fois les données supprimées, vous recevrez une notification en tant que prestataire d'activités pour vous confirmer que la suppression des données a bien été effectuée. Les coordonnées supprimées, telles que le nom, l'adresse e-mail et le numéro de téléphone du client seront remplacées par la mention [Supprimé] sur FareHarbor.

## CCPA

La CCPA est une loi californienne qui garantit aux résidents de Californie le droit de savoir quelles informations personnelles sont collectées à leur sujet, si elles sont vendues ou divulguées et à qui, d'accéder à ces informations et de refuser leur vente, et de bénéficier de services et de tarifs égaux même lorsqu'ils exercent leurs droits en matière de protection de la vie privée.

Pour en savoir plus sur la manière dont nous nous conformons à la CCPA et sur la manière dont vous pouvez exercer vos droits, veuillez consulter notre [Charte de confidentialité](#).

## Conformité PCI

Toute entreprise qui traite, stocke ou transmet des données de cartes de crédit a l'obligation d'adhérer à la Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS). Chez FareHarbor, nous prenons très au sérieux la sécurité des cartes de paiement. Nous nous conformons à la norme PCI, qui s'applique à tous les paiements traités via nos systèmes. En outre, FareHarbor ne stocke aucune donnée relative aux titulaires de cartes. Tous les paiements collectés par FareHarbor sont traités par des prestataires de services certifiés PCI niveau 1, tels que Stripe, PayPal ou Adyen.

FareHarbor publie chaque année un rapport PCI SAQ-D, qui est la façon la plus stricte de rendre compte de la conformité PCI. Ces exigences comprennent, sans s'y limiter :

- des analyses de sécurité trimestrielles effectuées par un prestataire de services d'analyse certifié PCI, et une surveillance constante des vulnérabilités ;
- le respect des normes du secteur rigoureuses en matière de chiffrement et de stockage des données ; le chiffrement de toutes les données pendant leur transit à l'aide du protocole TLS1.1 ou d'une version plus récente ;

- les meilleurs outils de sécurité pour nos systèmes, tels que la détection d'intrusion et la surveillance de l'intégrité des fichiers, et l'isolation de nos réseaux du reste d'Internet ;
- la formation de nos ingénieurs et nos employés à toutes les bonnes pratiques modernes en matière de cybersécurité.

### **Conformité de votre entreprise à la norme PCI.**

Toute entreprise impliquée dans le traitement des cartes de crédit doit se conformer aux exigences de la norme PCI DSS. Nombre d'entre elles sont déjà satisfaites par le simple fait d'utiliser FareHarbor. Toutefois, votre banque peut toujours exiger une certification attestant que vous vous conformez à la norme de sécurité PCI. Si FareHarbor est votre seul système de point de vente et que vous n'acceptez pas les paiements EMV, vous pouvez obtenir ce document facilement en remplissant un [PCI SAQ-A](#) et en le fournissant à votre banque.

Si vous acceptez les paiements EMV et/ou si FareHarbor n'est pas votre principal point de vente, il se peut que vous deviez vous conformer à d'autres directives. Veuillez envoyer un e-mail à l'adresse [security@fareharbor.com](mailto:security@fareharbor.com) pour planifier une session de découverte PCI ou pour toute question relative à la conformité PCI.

## **Sécurité organisationnelle et Infrastructure**

Tous les employés de FareHarbor reçoivent une formation sur l'importance de la protection de la vie privée et de la sécurité et doivent adhérer à une politique interne globale et inflexible en matière de sécurité et d'utilisation des données.

Les serveurs de FareHarbor fonctionnent dans les centres de données hautement sécurisés d'Amazon Web Services. L'application FareHarbor fonctionne dans un Cloud privé virtuel, chaque hôte étant protégé par des pare-feu configurés selon les règles les plus strictes. Toutes les communications avec FareHarbor sont protégées au niveau du réseau par des protocoles sécurisés de qualité industrielle. Une architecture sécurisée, de bonnes pratiques internes et des audits de tiers sont autant de composantes importantes de notre programme de sécurité.