La traduzione è fornita solo a scopo informativo. La versione definitiva di questa pagina è in inglese.

Panoramica sulla Sicurezza e sulla Privacy

La nostra missione presso FareHarbor è aiutarti a gestire e far crescere la tua attività con i migliori strumenti di prenotazione e logistica. Consideriamo la sicurezza e la privacy una delle nostre responsabilità più importanti quando si tratta di compiere tale missione. Ciascuna sezione di seguito illustra il nostro approccio per soddisfare o superare i requisiti di conformità relativi ai dati e alla sicurezza della tua azienda.

GDPR

Il GDPR (Regolamento generale sulla protezione dei dati) è lo standard sulla privacy dei dati nell'Unione Europea (UE) che disciplina la protezione dei dati personali dei residenti nell'UE. Per aiutarti a rispettare il GDPR, forniamo il seguente supporto:

Il diritto di essere informati.

Ti preghiamo di notare che, in qualità di fornitore di attività, sei il titolare del trattamento dati dei tuoi clienti e per legge devi fornire ai clienti informazioni su quali dati personali che li riguardano vengono raccolti, utilizzati, consultati o altrimenti elaborati e in quale misura i dati personali vengono o saranno elaborati da parte tua. "Elaborato" è una definizione molto ampia ai sensi del GDPR e comprende, tra l'altro, la raccolta, la registrazione, la strutturazione, l'archiviazione, l'adattamento, l'utilizzo, la cancellazione o la distruzione dei dati personali. Su richiesta, renderemo disponibili le informazioni da te richieste se possono essere riprodotte solo da noi, e ciò sarebbe necessario per adempiere ai tuoi obblighi GDPR.

Accesso ai dati, portabilità, rettifica e cancellazione.

Dopo la prenotazione, i tuoi clienti possono richiedere che i dati memorizzati vengano forniti e, se necessario, cancellati. Se invii un modulo tramite FareHarbor.com, puoi richiedere allo stesso modo che i tuoi dati memorizzati vengano forniti e, se necessario, eliminati. Le richieste di dati possono essere effettuate tramite il nostro Modulo di richiesta dati.

Tutte le richieste di dati vengono esaminate e autenticate dal personale addetto alla sicurezza. Per le richieste autenticate, i dati vengono cancellati entro 30 giorni. Una volta rimossi, ti verrà inviata una notifica, in qualità di fornitore dell'attività, per confermare che la rimozione dei dati è stata completata. I recapiti eliminati, come il

nome, l'indirizzo e-mail e il numero di telefono del cliente, appariranno come [Rimosso] all'interno di FareHarbor.

CCPA

Il CCPA è una legge della California che garantisce il diritto dei californiani di sapere quali dati personali vengono raccolti su di loro, di sapere se i loro dati personali vengono venduti o divulgati e a chi, di dire "no" alla vendita dei dati personali, di accedere ai propri dati personali e di ottenere la parità di servizio e di prezzo, anche se esercitano i propri diritti sulla privacy.

Per maggiori informazioni su come rispettiamo il CCPA e su come puoi esercitare i tuoi diritti, leggi la nostra Informativa sulla privacy.

Conformità PCI

Ogni azienda coinvolta nell'elaborazione, nell'archiviazione o nella trasmissione dei dati delle carte di credito deve rispettare gli standard di sicurezza dei dati del settore delle carte di pagamento. Noi di FareHarbor prendiamo molto sul serio la sicurezza delle carte di pagamento. FareHarbor è conforme allo standard PCI e ciò si estende a tutti i pagamenti elaborati tramite i nostri sistemi. Inoltre, FareHarbor non memorizza alcun dato del titolare della carta. Tutti i pagamenti riscossi tramite FareHarbor vengono elaborati da fornitori di servizi certificati PCI di livello 1, come Stripe, PayPal o Adyen.

FareHarbor redige annualmente un rapporto PCI SAQ-D (il metodo più rigoroso per segnalare la conformità PCI). Tali requisiti includono, ma non sono limitati a:

- Invio di scansioni di sicurezza trimestrali da parte di un fornitore di scansioni approvato da PCI e monitoraggio costante per individuare eventuali vulnerabilità.
- Rispetto di rigorosi standard di settore in materia di crittografia e archiviazione dei dati. Tutti i dati vengono crittografati durante il transito utilizzando TLS1.1 o una versione successiva.
- Dotazione dei nostri sistemi dei migliori strumenti di sicurezza, come il rilevamento delle intrusioni e il monitoraggio dell'integrità dei file, oltre all'isolamento delle nostre reti da Internet.
- Formazione dei nostri ingegneri e dipendenti su tutte le migliori pratiche moderne in materia di sicurezza informatica.

Conformità PCI della tua azienda

Ogni azienda coinvolta nell'elaborazione delle carte di credito deve rispettare i requisiti PCI DSS, anche se molti di essi saranno soddisfatti solo perché si utilizza FareHarbor. Tuttavia, la tua banca potrebbe comunque richiedere una certificazione che attesti la tua conformità allo standard di sicurezza PCI. Se FareHarbor è il tuo unico sistema di punto vendita e non accetti pagamenti con POS, puoi farlo facilmente compilando un PCI SAQ-A e fornendo tale documento alla tua banca.

Se accetti pagamenti con POS e/o FareHarbor non è il tuo punto vendita principale, potresti dover seguire linee guida diverse. Per programmare una sessione di individuazione PCI o per qualsiasi domanda sulla conformità PCI, scrivi all'indirizzo security@fareharbor.com.

Sicurezza organizzativa e infrastruttura

Tutti i dipendenti di FareHarbor sono formati sull'importanza della privacy e della sicurezza e devono aderire a una politica interna rigida e completa sulla sicurezza e sull'utilizzo dei dati.

FareHarbor viene eseguito nei data center altamente sicuri di Amazon Web Services. L'applicazione FareHarbor viene eseguita all'interno di un Virtual Private Cloud, con singoli host protetti da firewall configurati con le regole più rigorose. Tutte le comunicazioni con FareHarbor sono protette a livello di rete mediante protocolli sicuri e di livello industriale. Un'architettura protetta, le migliori pratiche interne e gli audit di terze parti sono tutti elementi importanti del nostro programma di sicurezza.