Vær oppmerksom på at oversettelsen kun er til informasjonsformål. Den gjeldende versjonen av denne siden er den engelske versjonen.

Oversikt over sikkerhet og personvern

Hos FareHarbor er vårt mål å hjelpe deg med å administrere og utvide virksomheten din med de beste booking- og logistikkverktøyene i bransjen. Vi anser sikkerhet og personvern som våre viktigste forpliktelser på veien mot dette målet. Hvert avsnitt nedenfor beskriver hvordan vi jobber for å oppfylle eller overgå kravene til samsvar med hensyn til virksomhetens data og sikkerhet.

Personvernforordningen

Personvernforordningen er personvernstandarden i Den europeiske union (EU) som regulerer beskyttelsen av personopplysninger for innbyggere i EU. For å hjelpe deg med å overholde personvernforordningen tilbyr vi følgende støtte:

Retten til å bli informert.

Vær oppmerksom på at du som aktivitetsleverandør er behandlingsansvarlig for kundens opplysninger, og at du derfor er lovpålagt å gi kundene informasjon om hvilke personopplysninger om dem som samles inn, brukes, konsulteres eller behandles på annen måte, og i hvilken grad personopplysningene behandles eller vil bli behandlet av deg. «Behandlet» er en svært bred definisjon i personvernforordningen og omfatter blant annet innsamling, registrering, strukturering, lagring, tilpasning, bruk, sletting eller tilintetgjøring av personopplysninger. På forespørsel skal vi gjøre tilgjengelig opplysninger som du har bedt om, hvis disse opplysningene bare kan reproduseres av oss og dette er nødvendig for å oppfylle dine forpliktelser under personvernforordningen.

Tilgang til, portabilitet til, retting av og sletting av opplysninger.

Etter bookingen kan kundene dine be om å få utlevert og eventuelt slette de lagrede opplysningene sine. Hvis du sender inn et skjema via FareHarbor.com, kan du på samme måte be om å få utlevert og eventuelt slette de lagrede opplysningene dine. Forespørsler om opplysninger kan gjøres via vårt skjema for forespørsel om opplysninger.

Alle forespørsler om opplysninger blir gjennomgått og godkjent av sikkerhetsavdelingen. Opplysningene slettes innen 30 dager for godkjente forespørsler. Når opplysningene er fjernet, sendes det et varsel til deg som aktivitetsleverandør for å bekrefte at fjerning av

opplysninger er fullført. Slettet kontaktinformasjon, for eksempel kundens navn, e-postadresse og telefonnummer, vises som [Fjernet] i FareHarbor.

CCPA

CCPA er en californisk lov som sikrer californierne retten til å vite hvilke personopplysninger som samles inn om dem, til å vite om personopplysningene deres selges eller utleveres og til hvem, til å si nei til salg av personopplysninger, til å få tilgang til personopplysningene sine og til lik service og pris, selv om de benytter seg av personvernrettighetene sine.

Hvis du vil ha mer informasjon om hvordan vi overholder CCPA og hvordan du kan utøve dine rettigheter, kan du lese personvernerklæringen vår.

PCI-etterlevelse

Alle virksomheter som er involvert i behandling, lagring eller overføring av betalingskortopplysninger, må overholde Payment Card Industry Data Security Standards. Hos FareHarbor tar vi betalingskortsikkerhet på største alvor. FareHarbor er i samsvar med PCI, og det gjelder alle betalinger som behandles via systemene våre. I tillegg lagres ingen kortholderopplysninger av FareHarbor. Alle betalinger som samles inn gjennom FareHarbor, behandles av PCI Level 1-sertifiserte tjenesteleverandører, for eksempel Stripe, PayPal eller Adyen.

FareHarbor rapporterer årlig på en PCI SAQ-D (den strengeste måten å rapportere PCI-etterlevelse på). Disse kravene inkluderer, men er ikke begrenset til følgende:

- Gjennomgang av kvartalsvise sikkerhetsskanninger av en PCI-godkjent skanningsleverandør og kontinuerlig overvåking etter sårbarheter.
- Etterfølgelse av strenge bransjestandarder for kryptering og lagring av data. Alle data krypteres under overføring med TLS1.1 eller høyere.
- Utstyre systemene våre med de beste sikkerhetsverktøyene i bransjen, for eksempel innbruddsdeteksjon og filintegritetsovervåking, samtidig som vi isolerer nettverkene våre fra internettet.
- Opplæring av våre ingeniører og ansatte i alle moderne beste praksiser når det gjelder cybersikkerhet.

Din virksomhets PCI-etterlevelse

Alle virksomheter som er involvert i behandling av betalingskort, må overholde PCI DSS-kravene, og mange av dem vil være oppfylt bare fordi du bruker FareHarbor.

Banken din kan likevel kreve sertifisering av at du overholder PCI-sikkerhetsstandarden. Hvis FareHarbor er ditt eneste salgspunktssystem og du ikke godtar EMV-betalinger, kan dette vanligvis gjøres enkelt ved å fylle ut skjemaet PCI SAQ-A og levere det til banken din.

Hvis du godtar EMV-betalinger og/eller FareHarbor ikke er ditt primære salgspunkt, kan det hende du må rapportere i henhold til andre retningslinjer. Ta kontakt med security@fareharbor.com for å avtale en PCI-oppdagelsesøkt eller hvis du har spørsmål om PCI-etterlevelse.

Organisatorisk sikkerhet og infrastruktur

Alle FareHarbors ansatte får opplæring i viktigheten av personvern og sikkerhet, og de må følge ufravikelige og omfattende interne regler for sikkerhet og databruk.

FareHarbor kjører i Amazon Web Services' svært sikre datasentre. FareHarbor-applikasjonen kjører i en virtuell privat sky, med individuelle verter beskyttet av brannmurer som er konfigurert med de strengeste reglene. All kommunikasjon med FareHarbor er beskyttet på nettverksnivå ved hjelp av sikre protokoller i bransjekvalitet. En sikret arkitektur, intern beste praksis og tredjepartsrevisjoner er alle viktige komponenter i sikkerhetsprogrammet vårt.