Bitte beachten Sie, dass die Übersetzung nur zu Informationszwecken dient. Die maßgebliche Version dieser Seite ist die englische Version.

Überblick über Sicherheit und Datenschutz

Wir von FareHarbor haben es uns zur Aufgabe gemacht, Sie bei der Verwaltung und dem Wachstum Ihres Unternehmens mit den besten Buchungs- und Logistik-Tools zu unterstützen. Die Sicherheit und der Schutz der Privatsphäre gehören zu unseren wichtigsten Aufgaben, wenn es darum geht, diese Aufgabe zu erfüllen. In den folgenden Abschnitten wird unser Ansatz zur Erfüllung oder zum Übertreffen von Compliance-Anforderungen in Bezug auf die Daten und die Sicherheit Ihres Unternehmens erläutert.

DSGVO

Die DSGVO (Datenschutz-Grundverordnung) ist der Datenschutzstandard der Europäischen Union (EU), der den Schutz personenbezogener Daten von EU-Bürgern regelt. Um Sie bei der Einhaltung der DSGVO zu helfen, bieten wir Ihnen folgende Unterstützung an:

Das Recht auf Information.

Bitte beachten Sie, dass Sie als Aktivitätsanbieter für die Verarbeitung der Daten Ihrer Kunden als Datenverantwortlicher gelten und daher gesetzlich verpflichtet sind, die Kunden darüber zu informieren, welche sie betreffenden personenbezogenen Daten erhoben, verwendet, abgefragt oder anderweitig verarbeitet werden und in welchem Umfang diese personenbezogenen Daten von Ihnen verarbeitet werden oder werden sollen. Der Begriff „verarbeitet“ ist in der Datenschutz-Grundverordnung sehr weit gefasst und umfasst unter anderem die Erhebung, Aufzeichnung, Strukturierung, Speicherung, Anpassung, Verwendung, Löschung oder Vernichtung personenbezogener Daten. Auf Anfrage stellen wir die von Ihnen angeforderten Informationen zur Verfügung, wenn diese Informationen nur von uns reproduziert werden können und dies erforderlich ist, um Ihren Verpflichtungen aus der DSGVO nachzukommen.

Zugang, Übertragbarkeit, Berichtigung und Löschung von Daten.

Nach der Buchung können Ihre Kunden verlangen, dass ihnen ihre gespeicherten Daten zur Verfügung gestellt und ggf. gelöscht werden. Wenn Sie ein Formular über FareHarbor.com einreichen, können Sie ebenfalls verlangen, dass Ihre gespeicherten

Daten bereitgestellt und ggf. gelöscht werden. Datenanfragen können über unser Datenanfrageformular gestellt werden.

Alle Datenanfragen werden von der Sicherheitsabteilung überprüft und authentifiziert. Die Daten werden bei berechtigten Anfragen innerhalb von 30 Tagen gelöscht. Nach der Löschung erhalten Sie als Aktivitätsanbieter eine Benachrichtigung, die bestätigt, dass die Löschung der Daten abgeschlossen ist. Gelöschte Kontaktdaten, wie Name, E-Mail-Adresse und Telefonnummer des Kunden, werden bei FareHarbor als [Entfernt] angezeigt.

CCPA

Das CCPA ist ein kalifornisches Gesetz, das den Einwohnern Kaliforniens das Recht zusichert, zu erfahren, welche personenbezogenen Daten über sie gesammelt werden, zu erfahren, ob und an wen ihre personenbezogenen Daten verkauft oder weitergegeben werden, dem Verkauf personenbezogener Daten zu widersprechen, auf ihre personenbezogenen Daten zuzugreifen und den gleichen Service und Preis zu erhalten, auch wenn sie ihre Datenschutzrechte ausüben.

Weitere Informationen darüber, wie wir das CCPA einhalten und wie Sie Ihre Rechte ausüben können, finden Sie in unserer Datenschutzerklärung.

PCI-Einhaltung

Jedes Unternehmen, das an der Verarbeitung, Speicherung oder Übertragung von Kreditkartendaten beteiligt ist, muss sich an die Standards der Branche für Zahlungsdienstleister („Payment Card Industry Data Security Standards“) halten. Bei FareHarbor nehmen wir die Sicherheit von Zahlungskarten sehr ernst. FareHarbor arbeitet PCI-konform; dies gilt für alle Zahlungen, die über unsere Systeme abgewickelt werden. Außerdem werden von FareHarbor keine Karteninhaberdaten gespeichert. Alle Zahlungen, die über FareHarbor getätigt werden, werden von Dienstleistern, die nach PCI-Level-1 zertifiziert sind (wie Stripe, PayPal oder Adyen) verarbeitet.

FareHarbor berichtet jährlich über einen PCI SAQ-D (die gründlichste Art, über die Einhaltung der PCI-Richtlinien Bericht zu erstatten). Diese Anforderungen umfassen unter anderem:

- Vierteljährliche Sicherheits-Scans durch einen PCI-zugelassenen Scanning-Anbieter und ständige Überprüfung auf Schwachstellen.
- Einhaltung strenger Branchenstandards für die Verschlüsselung und Speicherung von Daten. Alle Daten werden bei der Übertragung mit TLS1.1 oder höher verschlüsselt.

- Ausstattung unserer Systeme mit den besten Sicherheitstools wie Eindringungserkennung und Dateiintegritätsüberwachung und Isolieren unsere Netzwerke vom Internet.
- Schulung unserer Entwickler und Mitarbeiter in allen modernen bewährten Verfahren zur Cybersicherheit.

PCI-Einhaltung durch Ihr Unternehmen

Jedes Unternehmen, das in die Verarbeitung von Kreditkartendaten involviert ist, muss die PCI-DSS-Anforderungen erfüllen, wobei viele davon bereits dadurch erfüllt werden, dass Sie FareHarbor verwenden. Es kann jedoch vorkommen, dass Ihre Bank dennoch eine Bescheinigung darüber verlangt, dass Sie den PCI-Sicherheitsstandard einhalten. Wenn FareHarbor Ihre einzige Verkaufsstelle ist und Sie keine Zahlungen am POS-Kassensystem akzeptieren, kann dies in der Regel einfach durch das Ausfüllen eines PCI-SAQ-A-Formulars und die Bereitstellung dieses Dokuments an Ihre Bank erfolgen.

Wenn Sie Zahlungen am POS-Kassensystem akzeptieren und/oder FareHarbor nicht Ihre einzige Verkaufsstelle ist, müssen Sie möglicherweise nach anderen Richtlinien Bericht erstatten. Bitte wenden Sie sich an „security@fareharbor.com“, um einen Termin für eine PCI-Überprüfung zu vereinbaren oder wenn Sie Fragen zur PCI-Konformität haben.

Organisatorische Sicherheit und Infrastruktur

Alle Mitarbeiter von FareHarbor werden über die Bedeutung des Datenschutzes und der Sicherheit geschult und müssen sich an eine feste, umfassende interne Sicherheits- und Datennutzungsrichtlinie halten.

FareHarbor läuft über die hochsicheren Rechenzentren von Amazon Web Services. Die FareHarbor-Anwendung läuft in einer Virtual Private Cloud, wobei die einzelnen Hosts durch Firewalls geschützt sind, die nach den strengsten Regeln konfiguriert sind. Die gesamte Kommunikation mit FareHarbor ist auf der Netzwerkebene durch sichere Protokolle nach Branchenstandard geschützt. Eine sichere Architektur, interne bewährte Verfahren und Audits durch Dritte sind wichtige Bestandteile unseres Sicherheitsprogramms.