verifone

PCI

All organisations involved with the processing, transmission or storage of card data must comply with the Payments Card Industry Security Standards (PCI DSS). The platform is certified as a PCI level 1 Service Provider. This is the highest level of certification available. Every 12 months this certification is renewed.

PCI compliancy only applies to card processing, not to alternative payment methods (APMs) like Google Pay.

The different integration methods have different requirements surrounding PCI compliancy. You will need to adhere to the PCI DSS Self-Assessment Questionnaires (SAQs). There are a few different levels of SAQs that are required for each integration method. Please review this document to ensure you are aware of the requirements for PCI compliancy.

An overview of the applicable SAQs for the API, Checkout and Inject integration methods:

Note: PCI Scope applies only to the tokenization of cards. Example: A card tokenized through Checkout and than used in an API call for a transaction has to comply with SAQ A.

Integration method	PCI Compliancy Requirement	Description
API	SAQ D	Merchants that have a website that directly receives and transmits cardholder data.
Checkout	SAQ A	Card-not-present merchants (e-commerce or mail/telephone-order), that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises.
Inject	SAQ A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of cardhodler data on merchant's systems or premises.