

PCI DSS (Payment Card Industry Data Security Standard)

Der PCI-Datensicherheitsstandard wurde entwickelt, um die Datensicherheit bei der Abwicklung von Kreditkartenzahlungen weltweit zu verbessern.

Der Payment Card Industry Data Security Standard, üblicherweise abgekürzt mit PCI, ist ein Regelwerk im Zahlungsverkehr, das sich auf die Abwicklung von Kreditkartentransaktionen bezieht. Die PCI Standards sind aus Sicherheitsstandards von Visa und MasterCard hervorgegangen und werden mittlerweile von allen namhaften Kreditkartenorganisationen unterstützt.

Handelsunternehmen und Dienstleister, die Kreditkarten-Transaktionen speichern, übermitteln oder abwickeln, müssen die Regelungen erfüllen. Halten sie sich nicht daran, können Strafgebühren verhängt, Einschränkungen ausgesprochen oder ihnen letztlich die Akzeptanz von Kreditkarten untersagt werden.

PA DSS

Der Payment Application Data Security Standard, kurz PA DSS, beschreibt die einzuhaltenden Sicherheitsrichtlinien für die einzelnen Teile eines gesamten Zahlungssystems. Die Einhaltung dieser Richtlinien ist Voraussetzung, falls eine PCI-Abnahme gemacht werden soll oder muss.

Für **eIPAY payment** allein kann es keine PCI-Abnahme geben, da es nur Teil eines gesamten Systems (Zahlungssystems) ist.

- Das vollständige System muss die PCI-Richtlinien einhalten, falls eine PCI-Abnahme erforderlich ist, da die durch die Sicherheitsrichtlinien zu schützenden Daten in allen Teilen des Gesamtsystems geschützt sein müssen.
- Jede Teilanwendung im Gesamtsystem muss die im PA DSS beschriebenen Sicherheitsrichtlinien einhalten.

eIPAY payment ist PA DSS konform, bietet also seinen Teil der Voraussetzungen für eine PCI-Abnahme für das vollständige System.

Mindestanforderung an Softwarelösungen, die **eIPAY payment** integriert haben:

- Die Ergebnisdatei „Outfile“ muss durch Ihre Software sicher gelöscht werden.

Welche Daten sind betroffen?

Welche Daten wie gespeichert werden dürfen, ist in der folgenden Tabelle aufgeführt:

	Datenelement	Speichern zulässig	Schutz erforderlich	PCI DSS Anf. 3.4
Karteninhaberdaten	Primary Account Number (PAN)	Ja	Ja	Ja
	Name des Karteninhabers ¹	Ja	Ja ¹	Nein
	Servicecode ¹	Ja	Ja ¹	Nein
	Ablaufdatum ¹	Ja	Ja ¹	Nein
Vertrauliche Authentifizierungsdaten ₂	Vollständige Magnetstreifendaten ³	Nein	Nicht zutr.	Nicht zutr.
	CAV2/CVC2/CVV2/CID	Nein	Nicht zutr.	Nicht zutr.
	PIN/PIN-Block	Nein	Nicht zutr.	Nicht zutr.

1 Diese Datenelemente müssen geschützt werden, wenn sie in Verbindung mit der PAN gespeichert werden. Dieser Schutz sollte gemäß den PCI DSS Anforderungen für den allgemeinen Schutz der Karteninhaberdaten-Umgebung erfolgen. Darüber hinaus kann eine andere Gesetzgebung (z. B. im Zusammenhang mit dem Schutz persönlicher Verbraucherdaten, Datenschutz, Identitätsdiebstahl oder Datensicherheit) einen besonderen Schutz dieser Daten oder die ordnungsgemäße Weitergabe der Verfahren eines Unternehmens erfordern, wenn im Rahmen der Ausübung der geschäftlichen Tätigkeiten verbraucherbezogene persönliche Daten erfasst werden. PCI DSS gilt jedoch nicht, wenn PANs nicht gespeichert, verarbeitet oder übertragen werden.

2 Vertrauliche Authentifizierungsdaten dürfen nach der Autorisierung nicht gespeichert werden (auch wenn sie verschlüsselt wurden).

3 Vollständige Verfolgungsdaten vom Magnetstreifen, Magnetstreifenabbild auf dem Chip oder einem anderen Speicherort.

Wer benötigt eine PCI-Abnahme?

Eine PCI-Abnahme ist in erster Linie abhängig von der Anzahl der durchgeführten Transaktionen. In der folgenden Übersicht ist zu sehen, welche Unternehmen in welchem Umfang eine PCI-Abnahme benötigt:

Anzahl der Transaktionen pro Jahr	Standardtransaktionen/Mail/Phone Order-Transaktionen, E-Commerce-Transaktionen	Maßnahmen		
		Jährlich Vor-Ort Prüfung	Vierteljährlicher Sicherheitscheck	Selbstauskunft in Form eines Fragebogens
Mehr als 6 Mio.	Alle	Obligatorisch	Obligatorisch	
Weniger als 6 Mio.	Standardtransaktionen / Mail /Phone Order		Empfohlen	
Zwischen 20.000 und 6 Mio.	E-Commerce		Obligatorisch	Obligatorisch
Weniger als 20.000 Transaktionen	E-Commerce		Empfohlen	Empfohlen