Asperato are PCI-DSS Level One compliant, version 3.2.1.

We are externally assessed by a qualified QSA.

To request our Attestation of Compliance please email: support@asperato.com

---

Criminals are increasingly sophisticated in how they break into systems. It is, therefore, critical that merchants secure their systems to limit their exposure to account data compromises.

The Payment Card Industry Data Security Standard (PCI DSS) is a global set of security best practices which, when implemented correctly, will assist merchants in protecting their systems and help maintain the trust of their customers.

Asperato's approach to compliance and Salesforce

We don't just rely on encryption, meaning your administrators cannot access card details or bank details for that matter.

We ensure you receive 100% tokenized payment details. We don't ask you to store any sensitive cardholder data inside of Salesforce or within the Asperato application in the broader sense.

We ensure you can use all of Salesforce solutions, lightning components, automation, communities and more without falling foul of compliance.

All the elements of the Asperato package that do not reside in Salesforce and do handle sensitive data are externally assessed as being PCI DSS Level one compliant.

Considering an alternative supplier?

Ask for the following.

1. A copy of their Attestation of Compliance (AOC), it must be up to date and signed.
2. Validation of compliance is performed annually by either self-assessment or by an external Qualified Security Assessor (QSA). External validation is essential for level 1 compliance and highly recommended for level two.

Level 2 compliance is typically an indication that a solution is low volume. Be wary of self assessment that has not been externally assessed. If the provider is self assessed, always ask for penetration test results, scans and paperwork to support compliance.

What to ask your business.

Do we have our own PCI-DSS compliance?

You must ensure it is your companies compliance and not just that of an alternative solution provider, like a Payment Service Provider or e-commerce solution.

If no, you need it to process card payments.

If you do, make sure it will it cover all elements of payment processing journeys you are designing for Salesforce.

Common Claims / Assumptions

If I use a PCI-DSS Level One gateway API I am compliant?

No you are not. The gateway is just one small part of the compliance journey. You have to determine where any cardholder data is **processed** or **stored** and all of those systems, and anything that interacts with them, will be in scope for PCI-DSS compliance.

Salesforce is PCI-DSS compliant so I am too.

No, you are not. The Salesforce Attestation of Compliance is limited in its scope to the Salesforce infrastructure. It doesn't cover any application that is built on that infrastructure, nor the operation of that application.

Details here: https://help.salesforce.com/articleView?id=000175615&language=en_US&type=1

If we use the Encrypted Fields feature which is Level 1 PCI Compliant, we are ok right.

Not really. The Encrypted Fields feature in Salesforce is covered by the Salesforce Attestation of Compliance, but your use of it isn't. The moment you build an application that processes and/or stores cardholder data then you must conform to the PCI DSS requirements. The Salesforce compliance forms part of that program but it's not the answer by itself.

We embed PCI compliant payment processing capabilities (like paypages) directly from within Salesforce, built 100% on the Salesforce platform, we are ok right?

Probably wrong. A component (like encryption) itself doesn't make the overall application compliant.

Levels and compliance validation requirements

Level*	Merchant criteria	Validation requirements
1	Merchants processing more than six million transactions annually via all channels *or* global merchants identified as level one by any Visa region.	Annual Report on Compliance (ROC) to follow an on-site audit by either a Qualified Security Assessor (QSA) Quarterly network scan by Approved Scan Vendor (ASV) Attestation of Compliance form
2	Merchants processing one million to six million transactions annually via all channels.	Annual Self-Assessment Questionnaire (SAQ) Quarterly network scan by Approved Scan Vendor (ASV) Attestation of Compliance form