

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Before there was GDPR, before WCAG there was PCI Compliance.

If you collect and store personal financial information, you need to be compliant, both online and off. Here are the fundamentals, that make compliance less scary.

WHO NEEDS TO COMPLY?

It's simple, if your business collects and stores personal information, such as social security numbers, bank account numbers and/or credit card data you need to comply. At your business you need to lock that data up safely, and the same principles apply online.

HOW DO I COMPLY?

Compliance can be done in a self-service manner, there are no certified compliance vendors. However, there are online services and service providers that will walk you through the process for a fee. **Beware**, some of the online services can be tedious, onerous and confusing, even for tech professionals.

LESS IS BETTER

Generally speaking if you don't **need** to store personal financial data, just don't. It will reduce your exposure to theft & fraud, and makes compliance easy.

RESOURCES

PCI Compliance Official Website

<https://www.pcisecuritystandards.org>

Self Assessment Questionnaire

https://www.pcisecuritystandards.org/documents/SAQ_A_v3.pdf

