more security. usd

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS 4.0)

Introduction to the Standard

Classification: Public (V0)

Januar 2023

TABLE OF CONTENTS

REFERENCES
HEAR FROM OUR CLIENTS

equensWorldline

"It is crucial to have a reliable partner when it comes to highly complex projects such as the initial PCI DSS certification. usd supported us in each phase of the certification in a very competent way. In this context, it was especially important and pleasant to notice the very pragmatic and solution-oriented approach of the consultants. Therefore, solutions were found even for difficult problems. On the basis of our excellent first experience, we will continue to rely on usd as a partner for our re-certifications".

Thomas Maaß

Director Banking & Finance Central Europe

Eurowings

"Our customers' data security is our top priority. PCI DSS plays an important strategic role in this. We are glad to have such a strong partner in usd AG, who supported us in validating our compliance with PCI DSS".

Mehtap Secilmis

Head of IT Governance and Information Security Officer Eurowings Group

zalando

"I am really happy about this joint project. The certification process was uncomplicated and necessary measures could quickly be implemented thanks to the close cooperation between Zalando teams and usd. For us, this is an important step that shows that we always have the security of our customers' data in mind, even with agile and fast product development. This project proves it".

Benjamin Pannier

Managing Director
Zalando Payments GmbH

PCI DSS
PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Payment card data is a very sought-after target for criminals. In many cases, it can easily be stolen, especially from smaller companies, and turned into money with relatively little effort. Whether the attacks are carried out by professional hackers or malicious insiders: the criminals are usually highly organized, and the business with stolen payment card information is flourishing.

Discovery of theft of payment card information initially leads to a series of costly investigations. These investigations are followed by claims for damages and penal fines. Finally, publication of the incident by the press results in a loss of reputation from which a company can only recover with great effort. Custom-er confidence dwindles and your business suffers lasting damage.

This is why in October 2004, the payment card industry founded the Payment Card Industry Security Standards Council (PCI SSC) which developed the worldwide valid PCI Data Security Standard (PCI DSS) by standardizing the security guidelines of the individual payment card schemes.

The PCI DSS is based on best practices and is continuously updated to counter current threats. It provides the basis for a standardized approach to protecting payment card data and includes both technical and organizational measures. If these measures are implemented, their combined effects provide a minimum level of security of payment card data.

Validating your company's compliance with the PCI DSS can significantly influence the question of liability if a case of a payment card theft is detected. However, you must provide evidence that you had imple-mented and complied with all measures specified by the PCI DSS at the time of the incident.

ABOUT usd AG

usd AG has been advising and certifying businesses worldwide according to the PCI SSC security standards since 2005. usd is officially accredited as a Qualified Security Assessor, Approved Scanning Vendor, Payment Application Qualified Security Assessor, Point-to-Point Encryption QSA and PCI 3DS Assessor and Qualified PIN Assessor.

2.1. THE MAIN TARGET OF CYBER CRIMINALS

The number one target for cyber criminals are not the physical cards themselves, but the payment card data.

Criminals are particularly interested in stealing these types of data:

- Cardholder name
- Expiry date
- Credit card number (PAN)
- Verification code (CVC2/CVV2/…)

This data is either printed on the card or stored on the chip and the magnetic strip. Once in possession of this data, criminals can make payments to the cardholder's expense – e.g. on the internet. In some cases, the payment card number alone (without card verification code) is sufficient to make a purchase. Credit card thieves often sell stolen data to others, e.g. through an organized black market for stolen credit card data on the internet. The criminals are usually highly organized and operate internationally. Since it is almost impossible to trace their activities, their risk of being caught is relatively low.

The measures imposed by the PCI DSS focus on securing potential attack channels and therefore offer a significant level of protection for payment card data.

2.2. PCI DSS COMPLIANCE

There is no legal obligation to comply with the PCI DSS. Companies that store, process or transmit credit card data must comply with the standard nevertheless. While compliance is not required by law, it is required by the payment card organizations themselves. These organizations demand regular validation of a company's PCI DSS compliance, i.e. proof that the company fulfills the security requirements defined in the standard.

Whether you are required to validate PCI DSS compliance ultimately depends on the contractual situation with your credit card processors, e.g. the a*cquirer (merchant bank)* or *payment service provider (PSP)*.

Most companies that come into contact with payment card data belong to the category of *merchants*. They accept payments by payment card in exchange for goods or services. Most companies that have concluded a payment card acceptance agreement are categorized as merchants.

Organizations that provide services to merchants or banks and process credit card data themselves or have access to this data are categorized as *service providers*. These include, for example, network operators, acquiring and issuing processors, web hosting providers for online portals or IT service providers that operate the server infrastructure or the corporate firewall for third parties.

PARTIES INVOLVED IN PAYMENT TRANSACTIONS IN THE CREDIT CARD INDUSTRY

2.3. COMPLIANCE MANDATES

The credit card organizations contractually oblige acquirers to ensure that an agreed minimum percentage of their merchants achieve PCI DSS compliance. The acquirers pass on this obligation to their merchants via the card acceptance agreement. The merchants, in turn, contractually oblige their service providers to be PCI DSS compliant and to provide proof of their compliance.

2.4. CLASSIFICATIONS & ASSESSMENT METHODS

Depending on their classification (level), merchants and service providers have to conduct different assessment procedures to achieve their PCI DSS certification. The levels for merchants and service providers are defined based on their annual card transaction volume for each payment card organizations.

The following classifications (levels) apply to merchants:

Level	American Express	MasterCard & Visa Europe
1	> 2.5 million transactions per year	> 6 million transactions per year
2	50,000 to 2.5 million transactions per year	1 million to 6 million transactions per year
3	< 50,000 transactions per year	20,000 to 1 million e-commerce transactions per year

Level	American Express	MasterCard & Visa Europe
4	–	E-commerce merchants processing less than 20,000 transactions per year
	–	Non-e-commerce merchants processing less than 1 million transactions per year

The following classifications (levels) apply to service providers:

Level	American Express	MasterCard & Visa Europe
1	>= 2.5 million transactions per year	>= 300,000 transactions per year
2	50,000 – 2.5 million transactions per year	< 300,000 transactions per year

The following requirements apply to merchants and service providers depending on their level:

Classification	Self-Assessment Questionnaire (SAQ)	PCI DSS Security Scans	PCI DSS On-site Assessment
Level 1 merchant	–	Quarterly	Annually
Level 2 merchant	Annually *	Quarterly	Annually
Level 3 merchant	Annually	Quarterly	–
Level 4 merchant	Annually	Quarterly	–
Level 1 service provider	–	Quarterly	Annually
Level 2 service provider	Annually	Quarterly	–

As an officially accredited assessor in the payment card industry, we support you in validating your PCI DSS compliance. Please find a detailed description of the above-mentioned assessment methods in the following chapters.

* Level 2 merchants usually receive their onsite assessment report in the form of a Self-Assessment Questionnaire (SAQ). On request, we also prepare a Report on Compliance (RoC) for merchants with this level.

WHY DOES **PCI DSS COMPLIANCE** MATTER?

In many cases of credit card theft, it is revelaed afterwards that one or more of the PCI DSS measures were not implemented at the time of the theft. Numerous studies have shown that

MORE THAN
3/4
OF ATTACKS

could have been prevented with simple measures and little (financial) effort.

The implementation of PCI DSS requirements not only ensures a noticeably higher level of security throughout your company, but also creates significant added value, combined with the following advantages:

- You can identify risks associated with processing credit card and other customer informationen
- You demonstrate to your customers that you take the security of their data seriously
- You improve your protection against financial liability risks, legal costs and costs for the preservation of evidence
- You avoid negative press

2.5. THE PCI DSS REQUIREMENTS

The PCI DSS comprises a total of 6 control objectives, which are divided into 12 main requirements with a total of 329 individual requirements. The standard covers technical as well as organizational and documentary requirements.

Control Objective	Nr.	Chapter
Build and Maintain a Secure Network	1	Install and maintain network security controls
	2	Apply secure configurations to all system components
Protect Cardholder Data	3	Protect stored cardholder data
	4	Encrypt transmission of cardholder data and other sen-sitive information across open, public networks
Maintain a Vulnerability Management Program	5	Protect all systems and networks from malicious software
	6	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7	Restrict access to system components and carholder data by business need to know
	8	Identify users and authenticate access to system components
	9	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10	Log and monitor all access to system components and cardholder data
	11	Regularly test security systems and processes
Maintain an Information Security Policy	12	Support information security with organizational policies and programs

By implementing the PCI DSS, you raise your company's security level as a whole and contribute significantly to the protection of credit card data.

YOUR CONTACT

Would you like to know more about our services or products? Our sales team is happy to answer your questions on the phone or by e-mail.

Anna-Magdalena Kohl
usd Sales Representative, PCI Professional

Phone: +49 6102 8631–190 | Email: sales@usd.de
PGP oder S/MIME for encrypted communication