

Payment Card Industry Data Security Standard – PCI DSS

PCI DSS is a global standard for a safer handling of credit card data. The standard is a comprehensive set of requirements to which all parties that store, submit, or process card data, must adhere to and comply with. The aim of PCI DSS is to minimize the risk of compromise and theft of card data, and to strengthen confidence in cards as a mean of payment. The standard was developed by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International.

Validation of compliance with PCI DSS requirements is mandated by MasterCard and Visa, and is applicable to all Euroline's merchants. Non compliance will expose your business to a great financial risk and may ultimately result in the loss of right to accept card payments. As a Euroline merchant, we will provide you with the necessary tools to guide your business towards PCI DSS compliance. For more detailed and updated information on this global standard, please visit www.pcisecuritystandards.org

We hereby aim to give our Airline and E-commerce merchants a guide to Euroline's policy and present the available options and the implications of each with regard to PCI DSS. Our general recommendation is to minimize storage, submission or processing of cardholder data.

E-commerce

Eurolines' e-commerce merchants must use a PCI DSS certified Payment Service Provider (PSP) and choose a hosted solution. Hence all handling of card data is to be outsourced to a certified third party, thereby eliminating:

- risk of being compromised
- financial exposure
- time consuming and costly investments to upgrade/replace current systems

In the event a merchant must store, transmit or process any cardholder data on their premises, Euroline may grant exemption in which case the requirement is that merchant validate compliance by:

- Answering PCI DSS Self-Assessment Questionnaire (SAQ) variant D (app. 220 questions) <https://www.pcisecuritystandards.org/tech/instructions.htm>
- Performing network security scans regularly by an Approved Scanning Vendor (ASV*)
- Carrying out necessary changes upon completion of the above.

This requires a continuous effort from merchant to work towards and validate compliance, and the risk it poses upon the merchant and Euroline, will be subject to Risk Committee review.

Airlines

We are aware of the fact that working towards compliance with PCI DSS is a complex and long-term project for the majority within the airline industry. In some cases the estimated time span to fully achieve compliance is set to several years, depending on existing solutions and complexity of the IT-environment in which card handling is carried out. Additionally, in order for merchants to be considered fully compliant with the standard, *all* parties through which card data is handled (agents, BSP's, PSP's etc.) *has to be* PCI DSS-certified.

However, validation of compliance is mandatory for all of Euroline's Airline merchants regardless of existing solutions or card acquiring volumes. The validation procedure can be summed up as following, where the merchant has to:

- Answer PCI DSS Self-Assessment Questionnaire (SAQ) variant D (app. 220 questions) <https://www.pcisecuritystandards.org/tech/instructions.htm>
- Perform network security scans regularly by an Approved Scanning Vendor (ASV*)
- Carry out necessary changes upon completion of the above.

In order to provide our merchants with adequate aid and resources, Euroline has entered a partnership agreement with Trustwave, the leading provider of information security and compliance management solutions. TrustKeeper® is a web based tool, developed by Trustwave, which guides merchants towards compliance with the PCI DSS requirements. Thanks to our agreement with Trustwave, we are able to offer a powerful tool to a reduced cost.