Duty to comply with the PCI DSS

As of the 1st of April 2024, all merchants should fully comply with the PCI DSS standard (currently in version 4.0).

1. Criteria for determining how to validate PCI DSS compliance

Merchant Level 1	**Validation methods of PCI DSS compliance**
> Annual number of transactions - over 6 million in the Visa or Mastercard system > Other high-risk merchants designated by a decision of the payment systems	> Annual **PCI DSS on-site assessment** > Quarterly **ASV Scanning**
Merchant Level 2	
> Annual number of transactions - from 1 to 6 million in the Visa or Mastercard system	> Annual **Self-Assessment Questionnaire*** > Quarterly **ASV Scanning**
Merchant Level 3	
> Annual number of eCommerce transactions - from 20 thousand to 1 million in the Visa or Mastercard system	> Annual **Self-Assessment Questionnaire** > Quarterly **ASV Scanning (if applicable)**
Merchant Level 4	
> Other Merchants	> Annual **Self-Assessment Questionnaire** (only at the request of the acquirer) > Quarterly **ASV Scanning** (if applicable and only at the request of the acquirer)

* Merchants who meet the criteria of SAQ A, A-EP, and/or D (see paragraph 4 below) must use the services of a QSA (Qualified Security Assessor) / ISA (Internal Security Assessor) as part of Compliance Self-Assessment Questionnaire and/or on-site assessment. Merchants who meet the criteria of SAQ B, B-IP, C, C-VT and/or P2PE can optionally use the services of the QSA / ISA, i.e. to complete the SAQ Self-Assessment Questionnaire.

2. PCI DSS compliance validation methods listed above:

> PCI DSS on-site assessment – PCI compliance assessment performed by an external Qualified Security Assessor (QSA – Qualified Security Assessor).

> A list of companies offering QSA services in Poland is available on the PCI DSS website:

- https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors.
- Self-Assessment Questionnaire (SAQ) (details under item 4).
- ASV Scanning (details under item 3)

3. ASV Scanning

- The external vulnerability network scanning is performed by companies designated by PCI DSS. The list of such companies (ASV – Approved Scanning Vendors) is available on the PCI DSS website: https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors.

4. Annual Self-Assessment Questionnaire (SAQ)

The type of SAQ questionnaire to be completed depends on the technological solutions used by the Merchant:

Description of the technology solutions used by the Merchant	**Type of SelfAssessment Questionnaire - SAQ**
A Merchant who conducts transactions without the physical presence of a payment card (eCommerce or MO/TO) and who entrusts the whole processing of the payment card data to an external service provider with a PCI DSS certificate, whereas the Merchant does not store payment card data in electronic form, does not send them nor process them in their IT systems or on their premises. (This does not apply to cases when the Merchant accepts payments in the presence of the cardholder.)	**A**
A merchant accepting transactions via the Internet (eCommerce) who entrusts the whole processing of the payment card data to an external service provider with a PCI DSS certificate, whereas the Merchant does not store payment card data in electronic form, does not send them nor process them in their IT systems or on their premises, and does not collect payment card data via their website, however, the level of security of this website may affect the security of transactions made with a payment card. (Applies only to cases where the Merchant accepts Internet payments.)	**A-EP**

A Merchant using only: • Devices of the Imprinter type and / or • standalone terminals connected via fixed-line telephone services, whereas the Merchant does not store payment card data in electronic form. (Does not apply to cases where the Merchant accepts online payments).	**B**
A Merchant using only standalone PCI-PTS certified terminals that connect using the IP protocol, without storing payment card data in electronic form. (Does not apply to cases where the Merchant accepts online payments).	**B-IP**
A Merchant who uses a payment application based on an IT system connected to the Internet. The Merchant does not store payment card data in electronic format. (Does not apply to cases where the Merchant accepts online payments).	**C**
A Merchant who enters transactions manually into a virtual terminal hosted on the Internet and managed by an external service provider that is PCI DSS certified. The Merchant does not store payment card data in electronic format. (Does not apply to cases where the Merchant accepts online payments).	**C-VT**
A Merchant using only standalone terminals that use and are managed by a PCI SSC-approved P2PE solution. The Merchant does not store payment card data in electronic format. (Does not apply to cases where the Merchant accepts online payments).	**P2PE**
Merchants using a commercial off-the-shelf mobile device (for example, a phone or tablet) with a secure card reader included on PCI SSC's list of validated SPoC Solutions. No access to clear-text account data and no electronic account data storage. (Do not apply to unattended card-present, mail-order/telephone order (MOTO), or ecommerce channels).	**SPoC**
All other Merchants with access to cardholder data and/or not belonging to any of the categories listed above.	**D**

> The SAQ types are available at: https://www.pcisecuritystandards.org/document_library?category=saqs#results.

> Merchant Level 2, Merchant Level 3, and Merchant Level 4 Merchants can fill out the SAQ form themselves. Merchant Level 2 Merchants must complete the SAQ form (and/or may perform the on-site audit) with the help of a QSA or one of their staff who has received the title of Internal Security Assessor (ISA) only and exclusively in the case of SAQ A, A-EP and D. How to qualify as ISA? - see the PCI DSS website: https://www.pcisecuritystandards.org/program_training_and_qualification/internal_security_assessor_c ertification.

5. The necessary information concerning PCI DSS

> PCI DSS document to be downloaded in the current version of the standard: https://www.pcisecuritystandards.org/document_library.

> PCI DSS - educational materials for Merchants and Service Providers: https://www.pcisecuritystandards.org/pci_security/educational_resources

> PCI DSS – SAQ forms and SAQ instructions/ Guidelines on how to complete them: https://www.pcisecuritystandards.org/document_library?category=saqs#results.

> PCI DSS – QSA companies: https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors.

> PCI DSS – ASV companies: https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors.

> PCI Council home page (PCI SSC): https://www.pcisecuritystandards.org/index.php.

> Source information from Mastercard: https://www.mastercard.us/en-us/business/overview/safety-and-security/security-recommendations/site-data-protection-PCI/merchants-need-to-know.html.

> Source information from VISA: https://usa.visa.com/support/small-business/security-compliance.html.