# Payment Card Industry
# Data Security Standard

---

# Attestation of Compliance for Report on Compliance – Service Providers

## Version 4.0.1

Publication Date: August 2024

# PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

**Entity Name: PayU Spolka Akcyjna (dba: PayU SA, PayU S.A, PayU SA Poland)**

**Date of Report as noted in the Report on Compliance: 29 May 2025**

**Date Assessment Ended: 28 May 2025**

# Section 1: Assessment Information

## Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures* ("Assessment"). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

## Part 1. Contact Information

### Part 1a. Assessed Entity (ROC Section 1.1)

| | |
|---|---|
| Company name: | PayU Spolka Akcyjna |
| DBA (doing business as): | PayU SA<br>PayU S.A.<br>PayU SA Poland |
| Company mailing address: | Ul. Grunwaldzka 186, Poznan, Poland. 60-166 |
| Company main website: | www.payu.com |
| Company contact name: | Szymon Jazy |
| Company contact title: | Chief Information Security Officer |
| Contact phone number: | +48 795 576 075 |
| Contact e-mail address: | szymon.jazy@payu.com |

### Part 1b. Assessor (ROC Section 1.1)

Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.

| | |
|---|---|
| PCI SSC Internal Security Assessor(s) | |
| ISA name(s): | Not Applicable. |
| Qualified Security Assessor | |
| Company name: | INTEGRITY360 EUROPE LIMITED |
| Company mailing address: | Termini, 3 Arkle Rd, Sandyford Business Park, Sandyford, Dublin 18, Ireland, D18 T6T7 |
| Company website: | www.integrity360.com |
| Lead Assessor name: | Yuriy Koshak |
| Assessor phone number: | +380 (93) 029 80 79 |

| | |
|---|---|
| Assessor e-mail address: | yuriy.koshak@integrity360.com |
| Assessor certificate number: | PCI QSA (206-328), PCI QPA (1300-207) |

## Part 2. Executive Summary

### Part 2a. Scope Verification

**Services that were INCLUDED in the scope of the Assessment (select all that apply):**

| | |
|---|---|
| Name of service(s) assessed: | Payment Gateway<br>Tokenization/vault services |

Type of service(s) assessed:

| **Hosting Provider:** | **Managed Services:** | **Payment Processing:** |
|---|---|---|
| ☐ Applications / software<br>☐ Hardware<br>☐ Infrastructure / Network<br>☐ Physical space (co-location)<br>☐ Storage<br>☐ Web-hosting services<br>☐ Security services<br>☐ 3-D Secure Hosting Provider<br>☐ Multi-Tenant Service Provider<br>☐ Other Hosting (specify):<br>Not Applicable. | ☐ Systems security services<br>☐ IT support<br>☐ Physical security<br>☐ Terminal Management System<br>☐ Other services (specify):<br>Not Applicable. | ☐ POI / card present<br>☒ Internet / e-commerce<br>☐ MOTO / Call Center<br>☐ ATM<br>☐ Other processing (specify):<br>Not Applicable. |
| ☐ Account Management | ☒ Fraud and Chargeback | ☒ Payment Gateway/Switch |
| ☐ Back-Office Services | ☐ Issuer Processing | ☐ Prepaid Services |
| ☐ Billing Management | ☐ Loyalty Programs | ☐ Records Management |
| ☒ Clearing and Settlement | ☐ Merchant Services | ☐ Tax/Government Payments |
| ☐ Network Provider | | |
| ☒ Others (specify): Card tokenization/vault services (when operating as a merchant) | | |

***Note:*** *These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.*

## Part 2. Executive Summary *(continued)*

### Part 2a. Scope Verification *(continued)*

**Services that are provided by the service provider but were NOT INCLUDED in the scope of the Assessment (select all that apply):**

| | |
|---|---|
| Name of service(s) not assessed: | Acquirer |

Type of service(s) not assessed:

| | | |
|---|---|---|
| **Hosting Provider:**<br>☐ Applications / software<br>☐ Hardware<br>☐ Infrastructure / Network<br>☐ Physical space (co-location)<br>☐ Storage<br>☐ Web-hosting services<br>☐ Security services<br>☐ 3-D Secure Hosting Provider<br>☐ Multi-Tenant Service Provider<br>☐ Other Hosting (specify):<br>Not Applicable. | **Managed Services:**<br>☐ Systems security services<br>☐ IT support<br>☐ Physical security<br>☐ Terminal Management System<br>☐ Other services (specify):<br>Not Applicable. | **Payment Processing:**<br>☐ POI / card present<br>☐ Internet / e-commerce<br>☐ MOTO / Call Center<br>☐ ATM<br>☐ Other processing (specify):<br>Not Applicable. |
| ☐ Account Management | ☐ Fraud and Chargeback | ☐ Payment Gateway/Switch |
| ☐ Back-Office Services | ☐ Issuer Processing | ☐ Prepaid Services |
| ☐ Billing Management | ☐ Loyalty Programs | ☐ Records Management |
| ☐ Clearing and Settlement | ☐ Merchant Services | ☐ Tax/Government Payments |
| ☐ Network Provider | | |
| ☒ Others (specify): Acquiring | | |

| | |
|---|---|
| Provide a brief explanation why any checked services were not included in the Assessment: | PayU performs some services as an acquiring member but these are considered outside the scope for this assessment. |

### Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

| | |
|---|---|
| Describe how the business stores, processes, and/or transmits account data. | PayU Spolka Akcyjna, PayU S.A., PayU SA Poland (hereafter PayU), is a Level 1 Service Provider, that provides a payment gateway service to their clients through a web-based / e-commerce transactions on behalf of merchants.<br>PayU collects the cardholder information, PAN, cardholder name, expiry date and CVV/CVC; which it uses to process payments through an acquirer channel. PayU provides this capability as a service to any online |

| | |
|---|---|
| | merchants who would like to receive payment for Card-Not-Present e-commerce transactions. |
| Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data. | Not Applicable. |
| Describe system components that could impact the security of account data. | AWS WAF, Feedzai (Anti-Fraud Platform) |

## Part 2. Executive Summary *(continued)*

### Part 2c. Description of Payment Card Environment

| | |
|---|---|
| Provide a high-level description of the environment covered by this Assessment.<br>*For example:*<br>• *Connections into and out of the cardholder data environment (CDE).*<br>• *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.*<br>• *System components that could impact the security of account data.* | PayU hosts their PCI DSS environment at 2 Datacenters in Poland.<br>The CDE consists of the Linux based Application, Data Base (Oracle managed) and management servers.<br>Network Security Controls are realized by Load Balancers (F5) and firewalls (Juniper).<br>Segmentation in PayU is implemented between data centers and office network via usage of VLANs, connections between the data centers are implemented via usage of IP SEC or MPLS tunnels. Office network is segmented in order to secure the CDE delivered by the third party (Allegro Group).<br>Connections to the CDE are provided only through a “jump station” accessible from a VLAN segmented from the rest of the office network. Access to the “jump station” is possible using multiple authentication methods since it is considered to provide remote access to the CDE.<br>Access controls based on IPA LDAP management, Okta with usage of 2FA mechanisms.<br>Security is controled using SOAR realized on the stack of Splunk, ElasticSearch and third-party applications, like CrowdStrike/ClamAV (AV solutions on workstations).<br>Traffic to Payment applications is controled via AWS WAF services. |
| Indicate whether the environment includes segmentation to reduce the scope of the Assessment.<br>(Refer to the “Segmentation” section of PCI DSS for guidance on segmentation) | ☒ Yes ☐ No |

### Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

| Facility Type | Total Number of Locations<br>(How many locations of this type are in scope) | Location(s) of Facility<br>(city, country) |
|---|---|---|
| *Example: Data centers* | *3* | *Boston, MA, USA* |
| Corporate Office | 1 | Poznan, Poland |
| Corporate Office | 1 | Warsaw, Poland |

| | | |
|---|---|---|
| Datacenter | 1 | Poznan, Poland |
| Datacenter | 1 | Krakow, Poland |
| | | |
| | | |

## Part 2. Executive Summary *(continued)*

### Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions*?

☐ Yes ☒ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

| Name of PCI SSC validated Product or Solution | Version of Product or Solution | PCI SSC Standard to which Product or Solution Was Validated | PCI SSC Listing Reference Number | Expiry Date of Listing |
|---|---|---|---|---|
| Not Applicable. | Not Applicable. | Not Applicable. | Not Applicable. | Not Applicable. |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website (www.pcisecuritystandards.org) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

## Part 2. Executive Summary *(continued)*

### Part 2f. Third-Party Service Providers
### (ROC Section 4.4)

For the services being validated, does the entity have relationships with one or more third-party service providers that:

| | |
|---|---|
| • Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage)) | ☒ Yes ☐ No |
| • Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers) | ☒ Yes ☐ No |
| • Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers). | ☒ Yes ☐ No |

**If Yes:**

| **Name of Service Provider:** | **Description of Services Provided:** |
|---|---|
| NEXI Central Europe a.s. | Payment gateway for transaction processing. |
| ZooZ Mobile LTD | Runtime environment backup connection solution to Visa and MC networks. |
| Allegro Group | Hosting Managed services (Collocation). |
| Feedzai | Anti-Fraud services. |
| Amazon Web Services, Inc. | Web Application Firewall (data shared during transition). AWS CloudFront only has access to HTTPS Tunnel, but not to data. |
| | |
| | |
| | |
| | |
| | |

***Note:*** *Requirement 12.8 applies to all entities in this list.*

## Part 2. Executive Summary *(continued)*

### Part 2g. Summary of Assessment (ROC Section 1.8.1)

*Indicate below all responses provided within each principal PCI DSS requirement.*

For all requirements identified as either "Not Applicable" or "Not Tested," complete the "Justification for Approach" table below.

***Note:*** *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

*Name of Service Assessed:* Card-not-present payment processing (internet/e-commerce), Tokenization/vault services (as merchant).

| **PCI DSS Requirement** | **Requirement Finding**<br>More than one response may be selected for a given requirement. Indicate all responses that apply. | | | | **Select If a Compensating Control(s) Was Used** |
|---|---|---|---|---|---|
| | **In Place** | **Not Applicable** | **Not Tested** | **Not in Place** | |
| Requirement 1: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 2: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 3: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 4: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 5: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 6: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 7: | ☒ | ☐ | ☐ | ☐ | ☐ |
| Requirement 8: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 9: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 10: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 11: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 12: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Appendix A1: | ☐ | ☒ | ☐ | ☐ | ☐ |
| Appendix A2: | ☐ | ☒ | ☐ | ☐ | ☐ |

### Justification for Approach

| | |
|---|---|
| For any Not Applicable responses, identify which sub-requirements were not applicable and the reason. | 1.2.6 N/A: There are no insecure services and protocols.<br>2.2.5 N/A: There are no insecure services, daemons or protocols.<br>2.3(2.3.1, 2.3.2) N/A: There are no wireless networks in scope.<br>3.3.1.1 N/A: Entity doesn't operate on card-present transactions.<br>3.3.1.3 N/A: Entity doesn't operate on card-present transactions.<br>3.3.3 N/A: The entity does not provide or support any issuing services.<br>3.4.2 N/A: There is no possibility for anyone to copy or relocate PAN data.<br>3.5.1.1 N/A: Hashing is not utilized for rendering PAN unreadable.<br>3.5.1.2, 3.5.1.3 N/A: Disk encryption is not used.<br>3.7.9 N/A: Entity does not share cryptographic keys with its customers.<br>4.2.1.2 N/A: There are no wireless networks in scope.<br>4.2.2 N/A: Full PANs are not used in communications via end-user messaging technologies.<br>5.2.3, 5.2.3.1 N/A: There are no system components that are not at risk for malware. Anti-malware solutions monitor all components of the CDE.<br>5.3.3 N/A: Utilization of removable media is prohibited.<br>6.4.1 N/A: Requirement is superseded by Requirement 6.4.2,<br>6.5.2 N/A: There have been no significant changes during the last 12 months.<br>8.2.2 N/A: Entity does not use group, shared or generic authentication credentials.<br>8.2.3 N/A: Entity does not have remote access to customer premises.<br>8.2.7 N/A: Third parties do not have access to CDE.<br>8.3.10 N/A: Requirement is superseded by Requirement 8.3.10.1.<br>9.4(9.4.1- 9.4.7) N/A: Entity is not using physical backup media.<br>9.5(9.5.1- 9.5.1.3) N/A: Entity is not managing card reading devices.<br>10.7.1 NA: Requirement is superseded by Requirement 10.7.2.<br>11.3.1.3 N/A: There have been no significant changes during the last 12 months.<br>11.3.2.1 N/A: There have been no significant changes during the last 12 month.<br>11.4.7 N/A: Entity is not a multi-tenant provider.<br>12.3.2 N/A: There are no any requirements met by entity with the Customized Approach.<br>12.5.3 N/A: There have been no significant changes during the last 12 months. |

| | |
|---|---|
| | A1 N/A: The entity is not a Shared Hosting provider.<br>A2 N/A: The entity does not serve card-present transactions. |
| For any Not Tested responses, identify which sub-requirements were not tested and the reason. | Not Applicable. |

## Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3**)

| | |
|---|---|
| Date Assessment began:<br>***Note:*** *This is the first date that evidence was gathered, or observations were made.* | 2025-03-26 |
| Date Assessment ended:<br>***Note:*** *This is the last date that evidence was gathered, or observations were made.* | 2025-05-28 |
| Were any requirements in the ROC unable to be met due to a legal constraint? | ☐ Yes ☒ No |
| Were any testing activities performed remotely? | ☒ Yes ☐ No |

# Section 3 Validation and Attestation Details

## Part 3. PCI DSS Validation (ROC Section 1.7)

**This AOC is based on results noted in the ROC dated** *(Date of Report as noted in the ROC 2025-05-29)*.

Indicate below whether a full or partial PCI DSS assessment was completed:

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one)***:**

☒ **Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby PayU Spolka Akcyjna has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.

☐ **Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements.

**Target Date** for Compliance: *YYYY-MM-DD*

An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.

☐ **Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.

This option requires additional review from the entity to which this AOC will be submitted.

*If selected, complete the following:*

| Affected Requirement | Details of how legal constraint prevents requirement from being met |
|---|---|
| | |
| | |
| | |

## Part 3. PCI DSS Validation *(continued)*

### Part 3a. Service Provider Acknowledgement

**Signatory(s) confirms:**
(Select all that apply)

| | |
|---|---|
| ☒ | The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein. |
| ☒ | All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects. |
| ☒ | PCI DSS controls will be maintained at all times, as applicable to the entity's environment. |

### Part 3b. Service Provider Attestation

| | |
|---|---|
| Signed by:<br>Krzysztof Gawronek<br>669B8C1BCB4949B... | Signed by:<br>Marcin Grześkowiak<br>CFA70C8CEC4D461... |
| *Signature of Service Provider Executive Officer* ↑ | Date: 2025-05-29 |
| Service Provider Executive Officer Name: Krzysztof Gawronek<br>Marcin Grześkowiak | Title: Member of the Board<br>Commercial Proxy |

### Part 3c. Qualified Security Assessor (QSA) Acknowledgement

| | |
|---|---|
| If a QSA was involved or assisted with this Assessment, indicate the role performed: | ☒ QSA performed testing procedures. |
| | ☐ QSA provided other assistance.<br>If selected, describe all role(s) performed: Not Applicable. |

| | |
|---|---|
| DocuSigned by:<br>Yuriy Koshak<br>CB0F6C0815CB470... | |
| *Signature of Lead QSA* ↑ | Date: 2025-05-29 |
| Lead QSA Name: Yuriy Koshak | |
| DocuSigned by:<br>ABA9DEC3FF57486... | |
| *Signature of Duly Authorized Officer of QSA Company* ↑ | Date: 2025-05-29 |
| Duly Authorized Officer Name: Martin Petrov | QSA Company: INTEGRITY360 EUROPE LIMITED |

### Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

| | |
|---|---|
| If an ISA(s) was involved or assisted with this Assessment, indicate the role performed: | ☐ ISA(s) performed testing procedures. |
| | ☐ ISA(s) provided other assistance.<br>If selected, describe all role(s) performed: Not Applicable. |

## Part 4. Action Plan for Non-Compliant Requirements

*Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.*

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

| **PCI DSS Requirement** | **Description of Requirement** | **Compliant to PCI DSS Requirements** (Select One) | | **Remediation Date and Actions** (If "NO" selected for any Requirement) |
|---|---|---|---|---|
| | | **YES** | **NO** | |
| 1 | Install and maintain network security controls | ☐ | ☐ | |
| 2 | Apply secure configurations to all system components | ☐ | ☐ | |
| 3 | Protect stored account data | ☐ | ☐ | |
| 4 | Protect cardholder data with strong cryptography during transmission over open, public networks | ☐ | ☐ | |
| 5 | Protect all systems and networks from malicious software | ☐ | ☐ | |
| 6 | Develop and maintain secure systems and software | ☐ | ☐ | |
| 7 | Restrict access to system components and cardholder data by business need to know | ☐ | ☐ | |
| 8 | Identify users and authenticate access to system components | ☐ | ☐ | |
| 9 | Restrict physical access to cardholder data | ☐ | ☐ | |
| 10 | Log and monitor all access to system components and cardholder data | ☐ | ☐ | |
| 11 | Test security systems and networks regularly | ☐ | ☐ | |
| 12 | Support information security with organizational policies and programs | ☐ | ☐ | |
| Appendix A1 | Additional PCI DSS Requirements for Multi-Tenant Service Providers | ☐ | ☐ | |
| Appendix A2 | Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections | ☐ | ☐ | |

*Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit:* *https://www.pcisecuritystandards.org/about_us/*