![PCI Security Standards Council logo]

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: Yandex Cloud Kazakhstan LLP

Date of Report as noted in the Report on Compliance: September 20, 2024

Date Assessment Ended: September 20, 2024

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:	Yandex Cloud Kazakhstan LLP
DBA (doing business as):	Yandex Cloud KZ
Company mailing address:	11/1 Al-Farabi Avenue, Bostandyk district, Almaty, 050059, Kazakhstan
Company main website:	yandex.cloud/ru-kz/
Company contact name:	Dmitriy Kudinov
Company contact title:	Head of compliance direction
Contact phone number:	+7 (965) 358-43-42
Contact e-mail address:	dimonk099@yandex-team.ru

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):	N/A

Qualified Security Assessor	
Company name:	Deiteriy Company Ltd.
Company mailing address:	Lasnamäe linnaosa, Peterburi tee 47, Tallinn, Harju maakond, 11415, Estonia
Company website:	deiteriylab.com
Lead Assessor name:	Victoria Gadalova
Assessor phone number:	+372 712 4616
Assessor e-mail address:	victoria.gadalova@deiteriy.com
Assessor certificate number:	205-900

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were <u>INCLUDED</u> in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	Infrastructure & Network:
	• Application Load Balancer (L7 load balancers);
	• Cloud DNS (Domain name management);
	• Cloud Logging (Yandex Cloud services logging);
	• Compute Cloud (Virtual machines and block storage);
	• Network Load Balancer (Network load balancers);
	• Object Storage (Scalable data storage);
	• Virtual Private Cloud (Cloud network management);
	• Monitoring (Collection and visualization of metrics).
	Containers:
	• Container Registry (Managed Docker images);
	• Managed Service for Kubernetes (Managed Kubernetes clusters).
	Security:
	• Identity and Access Management (Identification and access control to cloud resources);
	• Certificate Manager (TLS certificate management);
	• Key Management Service (Cryptographic keys management);
	• Lockbox (Create and store secrets);
	• Audit Trails (Collect and export audit logs).
	Data Platform:
	• Data Transfer (Data migration and transport tool);
	• Managed Service for PostgreSQL, ClickHouse, MySQL, Redis, OpenSearch, Apache Kafka, Greenplum, Prometheus;
	• Monitoring (Collection and visualization of metrics);
	• Object Storage (Scalable data storage).
	Serverless:
	• Object Storage (Scalable data storage).
	Resources & Operations:
	• Identity and Access Management (Identification and access control to cloud resources);
	• Cloud Logging (Yandex Cloud services logging);
	• Cloud Organization (Organization service management);
	• Monitoring (Collection and visualization of metrics);
	• Managed Service for Prometheus;
	• Resource Manager (Resource management in folders and clouds)
	• Yandex Cloud Console (Console for resource management).

Type of service(s) assessed:

Hosting Provider:	Managed Services:	Payment Processing:
☒ Applications / software	☐ Systems security services	☐ POI / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☒ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☒ Storage	☒ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services	Databases, analytics and container orchestration services	N/A
☒ Security services		
☐ 3-D Secure Hosting Provider		
☒ Multi-Tenant Service Provider		
☐ Other Hosting (specify):		
N/A		
☐ 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): N/A		

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 <u>NOT INCLUDED</u> in the scope of the Assessment (select all that apply):

Name of service(s) not assessed:	All other services not specifically listed above.

Type of service(s) not assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POI / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services	N/A	N/A
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (specify):		
N/A		
☐ 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): All other services not specifically listed above.

Provide a brief explanation why any checked services were not included in the Assessment:	All other services not specifically listed above were not included in the scope of the assessment by Company's management decision.

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.	The Company does not directly transmit, process or store cardholder data.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	The Company provides networking, computing, storage and security services that may be used to support the customers' solutions for storing, processing or transmitting cardholder data. The Company does not directly transmit, process, or store cardholder data in providing these services.

	Payments for the Company's services are made through Yandex Cloud Billing service (assessed separately).
	The Company's information infrastructure is hosted in the datacenter (assessed separately).
	The Company provides customers with controls and information needed to comply with PCI DSS.
Describe system components that could impact the security of account data.	The Company does not directly transmit, process or store cardholder data. However, next critical components can affect the security of account data:
	▪ Compute substrate including the host operating systems and hypervisors;
	▪ Compute instances excluding customer owned instances;
	▪ Compute instances used for services provided to customers;
	▪ firewalls and network devices;
	▪ applications provided to customers;
	▪ security services.

Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card Environment

Provide a high-level description of the environment covered by this Assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	The Company offers infrastructure, networking, application and security services that enable customers to create their own PCI DSS compliant information infrastructure. The Company does not directly transmit, process or store any cardholder data. Therefore, it considers that all customer data can be a cardholder data. The Company does not access customer data, except for troubleshooting and on a per incident basis with customer permission. All communications from out of scope and from the web application interfaces are performed through the secure protocols. The Company isolates the infrastructure in the scope of the assessment from office and other networks. The Company's infrastructure includes different critical components: ▪ Compute substrate including the host operating systems and hypervisors; ▪ Compute instances excluding customer owned instances; ▪ Compute instances used for services provided to customers; ▪ firewalls and network devices; ▪ applications provided to customers; ▪ security services.
Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (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 (How many locations of this type are in scope)	Location(s) of Facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
Corporate office	1	Almaty, Kazakhstan

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
N/A	N/A	N/A	N/A	N/A

---

*   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:
Yandex Cloud Kazakhstan LLP	Hardware hosting in the data center.

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:

Infrastructure & Network:

- *Application Load Balancer (L7 load balancers);*
- *Cloud DNS (Domain name management);*
- *Cloud Logging (Yandex Cloud services logging);*
- *Compute Cloud (Virtual machines and block storage);*
- *Network Load Balancer (Network load balancers);*
- *Object Storage (Scalable data storage);*
- *Virtual Private Cloud (Cloud network management);*
- *Monitoring (Collection and visualization of metrics).*

Containers:

- *Container Registry (Managed Docker images);*
- *Managed Service for Kubernetes (Managed Kubernetes clusters).*

Security:

- *Identity and Access Management (Identification and access control to cloud resources);*
- *Certificate Manager (TLS certificate management);*
- *Key Management Service (Cryptographic keys management);*
- *Lockbox (Create and store secrets);*
- *Audit Trails (Collect and export audit logs).*

Data Platform:

- *Data Transfer (Data migration and transport tool);*
- *Managed Service for PostgreSQL, ClickHouse, MySQL, Redis, OpenSearch, Apache Kafka, Greenplum, Prometheus;*
- *Monitoring (Collection and visualization of metrics);*
- *Object Storage (Scalable data storage).*

Serverless:

- *Object Storage (Scalable data storage).*

Resources & Operations:

- *Identity and Access Management (Identification and access control to cloud resources);*
- *Cloud Logging (Yandex Cloud services logging);*
- *Cloud Organization (Organization service management);*
- *Monitoring (Collection and visualization of metrics);*
- *Managed Service for Prometheus;*
- *Resource Manager (Resource management in folders and clouds)*
- *Yandex Cloud Console (Console for resource management).*

PCI DSS Requirement	Requirement Finding 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.	1.2.4, 1.4.4, 3.1 – 3.2.1, 3.4 – 3.5.1.3, 4.2.2, 6.5.5, 7.2.6, 10.2.1.1 – N/A, the Company does not directly store, process or transmit cardholder data and only provides hosting services to its clients.
	1.2.6 – N/A, there are no any insecure services, protocols and ports in use in the scope of the assessment.
	1.3.3, 2.3 – 2.3.2, 4.2.1.2 – N/A, there are no any wireless networks in the scope of the assessment.
	2.2.5 – N/A, there are no any insecure services, protocols and daemons in use in the scope of the assessment.
	3.3 – 3.3.2 – N/A, the Company does not directly store sensitive authentication data prior to completion of transaction authorization.
	3.3.3 – N/A, the Company is not an issuer and does not support issuing services.
	3.7.9 – N/A, the Company does not share keys with their customers for transmission or storage of account data.
	5.2.1, 5.2.2, 5.3 – 5.3.5 – N/A, the Company uses OS Linux in the scope of the assessment.
	5.2.3.1, 5.4 – 5.4.1, 6.4.2, 6.4.3, 7.2.4 – 7.2.5.1, 8.6.2, 8.6.3, 10.4.2.1, 10.7.2, 11.6 – 11.6.1, 12.3.1, 12.10.4.1, 12.10.5 – N/A, these future-dated requirements are not considered during the assessment.
	6.5.2 – N/A, no significant changes occurred in prior 12 months.
	7.2.6 – N/A, the Company does not have access to any customers repositories of stored cardholder data.
	8.2.3 – N/A, the Company does not have remote access to its customer premises.
	9.4.6 – N/A, there are no any hard-copy materials with cardholder data in the scope of the assessment.
	9.5.1 – 9.5.1.3 – N/A, there are no any devices that capture payment card data via direct physical interaction with the card in the scope of assessment.
	12.6.3.2 – N/A, there are no any end-user technologies in the scope of the assessment.
	Appendix A2 – the Company does not use any POS POI terminals in the scope of the assessment.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	N/A

Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3)

Date Assessment began: **Note:** *This is the first date that evidence was gathered, or observations were made.*	August 12, 2024
Date Assessment ended: **Note:** *This is the last date that evidence was gathered, or observations were made.*	September 20, 2024
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 September 20, 2024.

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 Yandex Cloud Kazakhstan LLP 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 N/A has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: N/A 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 N/A 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
N/A	N/A
N/A	N/A
N/A	N/A

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

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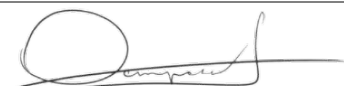
(Select all that apply)

☒ | 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

Signature of Service Provider Executive Officer ↑	Date: September 20, 2024
Service Provider Executive Officer Name: Dmitriy Kudinov	Title: Head of compliance direction

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. If selected, describe all role(s) performed: N/A

Signature of Lead QSA ↑	Date: September 20, 2024
Lead QSA Name: Victoria Gadalova	

Signature of Duly Authorized Officer of QSA Company ↑	Date: September 20, 2024
Duly Authorized Officer Name: Anton Ostrokonskiy	QSA Company: Deiteriy Company Ltd.

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. If selected, describe all role(s) performed: N/A

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/