Card Security

Opinion on Compliance of the Personal Data Protection System with the Requirements of Federal Law No. 152 "On Personal Data"

Card Security LLC

(Name of manufacturer and full name of an individual entrepreneur that accepted the declaration of compliance) (address, telephone, fax)

License for technical protection of confidential information No. 3099 dated November 22, 2016, issued by Federal Service for Technical and Export Control (FSTEC), represented by **CEO Alexander Yuryevich Ivanov**

(full name of CEO of an entity on behalf of which the declaration is accepted)

states that as a result of the audit of the personal data protection system of the "Yandex.Cloud Platform" Personal Data Information System (PDIS) for the Services specified in Appendix 1, hosted in the data centers:

- Yandex LLC, Silikatnaya str., 19, Mytishchi, Russia
- Yandex DC Vladimir LLC, Energetikov str., 37, Vladimir, Russia
- Yandex DC LLC, Pushkina str., 21, Sasovo, Russia

at the time of the compliance assessment, all necessary measures were taken to neutralize current threats for personal data security. Following the results of threat modeling, the third type threats were recognized as relevant, while the first type and second type threats were recognized as irrelevant. As of the compliance audit, all necessary measures were taken to neutralize the relevant personal data threats.

The above PDIS were found to be in compliance with the requirements of

1. **Federal Law No. 152 "On Personal Data" dated July 27, 2006**
2. **"Requirements for Protection of Personal Data Processed in Personal Data Information Systems" approved by Resolution of the Government of the Russian Federation No. 1119 dated November 1, 2012**
3. **"Scope and Contents of Technical and Organizational Measures for Ensuring the Security of Personal Data Processed in Personal Data Information Systems" approved by Order of FSTEC No. 21 dated February 18, 2013**

(regulatory documents complied with as confirmed by this declaration, with indication of paragraphs containing the requirements for the above products)

The "Yandex.Cloud Platform" PDIS ensures: **level 1 personal data protection.**

Appendix 2 provides a short summary of integrated protection mechanisms on the Yandex.Cloud Platform and protection measures which enable clients to comply with the requirements of the laws of the Russian Federation for level 3 personal data security.

Compliance declaration method**: on the basis of own evidence.**

Yandex.Cloud LLC has adopted the organizational and technical measures ensuring the compliance of Yandex.Cloud Platform PDIS with the requirements of Federal Law No. 152 "On Personal Data" and regulations thereunder.

Signed on **December 17, 2020**

L.S.

(Signature)

CEO of CardSec LLC A.Yu. Ivanov

(Initials, last name)

Card Security

Appendix No. 1 Services in “Yandex.Cloud Platform” PDIS audit scope

1.	Yandex Identity and Access Management
2.	Yandex Resource Manager
3.	Yandex Compute Cloud
4.	Yandex Virtual Private Cloud
5.	Yandex Load Balancer
6.	Yandex Object Storage
7.	Yandex Billing
8.	Yandex API Gateway
9.	Yandex Managed Service for (PostgreSQL, MySQL®, MongoDB, ClickHouse, Redis™, Apache Kafka®)
10.	Yandex DataProc
11.	Yandex Container Registry
12.	Yandex Cloud Functions
13.	Yandex IoT Core
14.	Yandex Managed Service for Kubernetes
15.	Yandex DataLens
16.	Yandex Database
17.	Yandex Marketplace
18.	Yandex Message Queue
19.	Yandex SpeechKit
20.	Yandex Translate

(Наименование, тип, марка продукции, на которую распространяется декларация, код ОК 005-93 и (или) ТН ВЭД СНГ)

Appendix No. 2 Allocation of Responsibility for Personal Data Protection

Requirement source	Measures to ensure the security of personal data	The Yandex.Cloud Platform's integrated protection mechanisms	Protection measures to be taken by clients to ensure level 3 security
Identification and authentication of access subjects and access objects (IA)			
IA.1	Identification and authentication of users who are the operator's employees	At the level of: • the Platform's physical hardware; • the system for controlling the virtualization environment; • the Platform's service servers and other virtual devices; • the Platform's services.	At the level of client's virtual machines and Docker containers
IA.2	Identification and authentication of devices, including stationary, mobile and portable devices	At the level of: • the Platform's physical hardware	N/A
IA.3	Identity management including the creation, assignment and destruction of IDs	At the level of: • the Platform's physical hardware; • the system for controlling the virtualization environment; • the Platform's service servers and other virtual devices; • the Platform's services.	At the level of client's virtual machines and Docker containers
IA.4	Management of authentication means including the storage, issue, initialization and blocking of authentication means and taking relevant measures in case of loss and/or compromising a means of authentication		
IA.5	Feedback protection during the input of authentication information		
IA.6	Identification and authentication of users who are not the operator's employees (external users)	At the level of access to the Platform's services provided to clients	At the level of client's virtual machines and Docker containers
Management of access by access subjects to access objects (MA)			
MA.1	Management (creation, activation, blocking and destruction) of user accounts including external users	At the level of: • the Platform's physical hardware; • the system for controlling the virtualization environment; • the Platform's service servers and other virtual devices; • the Platform's services.	At the level of client's virtual machines and Docker containers
MA.2	Implementation of necessary access control methods (discretionary, mandate, role-based or other method), types (reading, recording, execution or other type) and rules		

Requirement source	Measures to ensure the security of personal data	The Yandex.Cloud Platform's integrated protection mechanisms	Protection measures to be taken by clients to ensure level 3 security
MA.3	Management of information flows between devices (filtration, routing, connection control, one-way transmission and other management methods), segments of the information system and information systems	Management of network access at the level of: • the Platform's physical hardware; • the Platform's service networks; • access restriction between network segments of the Platform's different clients; • access restriction from client's network to the service network.	Managing network access: • between segments of client's virtual network; • to the client virtual network from outside it.
MA.4	Separation of powers (roles) of users, administrators and persons in charge of the information system's operation	At the level of: • the Platform's physical hardware; • the system for controlling the virtualization environment; • the Platform's service servers and other virtual devices; • the Platform's services	At the level of client's virtual machines and Docker containers
MA.5	Granting minimal necessary rights and privileges to users, administrators and persons in charge of the information system's operation		
MA.6	Limiting unsuccessful attempts to log in to the information system (access to the information system)		
MA.10	Blocking access session to the information system upon the expiry of a determined user's idle time (inactivity) or at the user's request		
MA.11	Authorization (ban) of user's acts permitted before identification and authentication		
MA.13	Implementation of protected remote access by access subjects to access objects through external information telecommunication networks	At the level of access by: • users to the Platform's services; • administrators to physical and virtual service system components.	At the level of remote access to client's virtual servers and Docker containers
MA.14	Regulation and control of usage of wireless access technologies in the information system	N/A	N/A
MA.15	Regulation and control of usage of mobile equipment in the information system	N/A	N/A
MA.16	Management of interaction with information systems of external organizations (external information systems)	At the level of the service system components	When organizing such interaction with client's virtual machines and Docker containers
MA.17	Providing trusted loading of computer equipment	At the level of the service system components	N/A
Software environment restrictions (SER)			
SER.2	Managing installation of software components, including defining components to be installed, configuring the installation parameters of components, and monitoring installation of software components .	At the level of: • physical Platform hardware; • Platform service/system servers and other virtual devices.	At the level of client's virtual machines and Docker containers
SER.3	Restrictions for only authorized software and/or installation of its components.	At the level of: • physical Platform hardware; • Platform service/system servers and other virtual	At the level of client's virtual machines and Docker containers

Requirement source	Measures to ensure the security of personal data	The Yandex.Cloud Platform's integrated protection mechanisms	Protection measures to be taken by clients to ensure level 3 security
		devices.	
Protection of machine media containing personal data (PMM)			
PMM.1	Accounting for machine media with personal data	At the level of physical data storage media used in the Platform	N/A
PMM.2	Access management for machine media with personal data	At the level of physical data storage media used in the Platform	N/A
PMM.8	Destruction (deletion) or depersonalization of personal data on machine-readable media when transferred between users or to external organizations for repair or disposal, as well as the control of destruction (deletion) or depersonalization	At the level of physical data storage media used in the Platform	N/A
Security event logging (SEL)			
SEL.1	Determining security events to be logged and their storage time	At the level of: • service system components; • the Platform's services including client's activities to use the services.	At the level of client's virtual servers and Docker containers, software and information protection means used therein.
SEL.2	Determining scope and contents of information about security events to be logged		
SEL.3	Collecting, recording and storing information on security events during the determined storage time		
SEL.5	Monitoring (viewing, analyzing) the results of registering security events and responding to them		
SEL.7	Protection of information on security events		
Virus protection (VP)			
VP.1	Implementation of virus protection	Not applicable, because the protected segment contains only the servers. The operating system used on servers is practically not subject to virus infection. There is no direct Internet access on servers and HIDS is used.	At the level of client's virtual machines and Docker containers.
VP.2	Updating the database of malware (virus) signatures		
Intrusion detection system (IDS)			
IDS.1	Intrusion detection	At the level of: • physical Platform hardware; • Platform service/system servers and other virtual devices.	At the level of client's network segments
IDS.2	Decision rule base update		
Control (analysis) of personal data security (AS)			
AS.1	Detection and analysis of the information system's vulnerabilities and prompt elimination of newly detected vulnerabilities	At the level of service virtual and physical system components	At the level of client's virtual machines and Docker containers
AS.2	Control of installation of software updates, including software updates for information protection means		
AS.3	Control of operability, settings and faultless operation of software and information protection means		

Requirement source	Measures to ensure the security of personal data	The Yandex.Cloud Platform's integrated protection mechanisms	Protection measures to be taken by clients to ensure level 3 security
AS.4	Control of composition of hardware, software and information protection means		
AS.5	Control of rules for generating and changing user passwords, creating and deleting user accounts, implementing access control rules, and user permissions in the information system		
Integrity of the information system and personal data (INT)			
INT.1	Software integrity control, including information security software	At the level of: • physical Platform hardware; • Platform service/system servers and other virtual devices.	At the level of client's virtual machines and Docker containers
INT.2	Detection and response to the receipt of unsolicited electronic messages (letters, documents) and other information that is not related to the functioning of the information system (spam protection)	Not applicable because the Platform does not provide functionality for electronic mail exchange.	At the level of client's mail servers
Availability of personal data (AVL)			
AVL.3	Monitoring of failure-free operation of hardware, detection and localization of failures of functioning, taking and testing measures to restore failed hardware	At the level of: • physical Platform hardware; • Platform service/system servers and other virtual devices. Automated data replication is performed in the platform storage.	At the level of the client's personal data system, backup and restoring personal data is performed by the client. At the level of client's virtual machines and Docker containers data backup is implemented using platform tools.
AVL.4	Periodic personal data backup on machine media reserved for personal data backups		
AVL.5	Ensuring the possibility of restoring personal data from machine media reserved for personal data backups (backup copies) within a specified time interval		
Virtualization environment protection (VEP)			
VEP.1	Identification and authentication of access subjects and access objects in virtual infrastructure including administrators of virtualization means	At the level of: • virtualization environment control means; • the Platform's service servers and other virtual devices; • the Platform's services.	N/A
VEP.2	Control of access by access subjects to access objects in virtual infrastructure including within virtual machines		At the level of client's virtual machines and Docker containers
VEP.3	Virtual infrastructure security events logging		
VEP.6	Managing the movement of virtual machines (containers) and data processed on them	At the level of: • virtualization environment control means; • the Platform's service servers and other virtual devices;	Implemented at the Platform architecture level
VEP.7	Control of virtual infrastructure and its configuration integrity	At the level of: • the Platform's service servers and other virtual devices	At the level of client's virtual machines and Docker containers
VEP.8	Data backup, backup of hardware and virtual infrastructure software, as well as communication channels within the virtual infrastructure	At the level of: • the Platform's service servers and other virtual devices;	At the level of client's virtual machines and Docker containers

Requirement source	Measures to ensure the security of personal data	The Yandex.Cloud Platform's integrated protection mechanisms	Protection measures to be taken by clients to ensure level 3 security
VEP.9	Implementation and management of virus protection in virtual infrastructure	Not applicable, because the protected segment contains only the servers. The operating system used on servers is practically not subject to virus infection. There is no direct Internet access on servers and HIDS is used.	At the level of client's virtual machines and Docker containers
VEP.10	Segmentation of virtual infrastructure for processing of personal data by a user and/or a group of users	Management of network access at the level of: • the Platform's service networks; • restriction of access between network segments of the Platform's different clients;	At the level of client's network segments
Protection of hardware (PH)			
PH.3	Control and management of physical access to: hardware, information protection means, operation support equipment and premises and buildings where they are installed to prevent unauthorized physical access to information processing equipment, information protection equipment and information system operation support equipment and to premises and buildings where they are installed	At the level of the data processing center's physical security protection	N/A
PH.4	Location of information output (display) devices preventing unauthorized viewing thereof	Output devices are not used in the data processing center to display personal data	N/A
PH.5	Protection against the external impacts (environmental impacts, interruptions of power supply, air conditioning and other external factors)	At the level of the data processing center	N/A
Protection of the information system, its equipment, communication and data transmission systems (PIS)			
PIS.1	Segregation of duties for the management (administration) of the information system, management (administration) of the personal data protection system, processing of personal data and other duties	At the level of: • the Platform's physical hardware; • virtualization environment control means; • the Platform's service servers and other virtual devices; • the Platform's services.	At the level of client's virtual machines and Docker containers
PIS.3	Protection of personal data against disclosure, modification and forcing (input of false information) during transferring (preparation for the transferring) thereof through communication channels which go beyond the controlled zone including wireless communication channels	At the level of the channels: • used for administrator's access to the Platform's system components; • used for the access of users and administrators to the virtualization environment control panel; • between data processing centers.	At the level of communication channels established by the client for access to the client's virtual machines

Requirement source	Measures to ensure the security of personal data	The Yandex.Cloud Platform's integrated protection mechanisms	Protection measures to be taken by clients to ensure level 3 security
PIS.11	Authenticity of network connections (interaction sessions), including protection against spoofing of network devices and services	At the level of channels: • used for administrators to access system components of the platform; • used for users and administrators to access the virtualization environment management console; • between data centers.	At the level of client's network segments
PIS.15	Archived files protection, protection of information security tools settings and software, and other data that cannot be changed during the processing of personal data	At the level of: • physical Platform hardware • Platform service/system servers and other virtual devices	At the level of client's virtual machines and Docker containers
PIS.17	Dividing the information system into segments (segmentation of the information system) and ensuring the protection of the perimeters of the information system segments	At the level of service/system network segments.	At the level of client's virtual network segments
PIS.20	Protection of wireless connections used in the information system	N/A	N/A
Identifying and responding to incident (IM)			
IM.1	Identification of persons responsible for identifying and responding to incidents.	From employees of Yandex.Cloud or its contractors	From employees of client organization or its contractors
IM.2	Incident detection, identification and registration	At the level of: • the Platform's physical hardware; • the system for controlling the virtualization environment; • Platform service/system servers and other virtual devices. • the Platform's services	At the level of client's virtual machines and Docker containers
IM.3	Promptly informing the persons responsible for identifying incidents and responding to them about the occurrence of incidents in the information system by users and administrators	From employees of Yandex.Cloud or its contractors	From employees of client organization or its contractors
IM.4	Incident analysis, including identification of sources and causes of incidents, as well as assessment of their consequences	At the level of: • the Platform's physical hardware; • the system for controlling the virtualization environment; • Platform service/system servers and other virtual devices. • the Platform's services	At the level of client's virtual machines and Docker containers
IM.5	Taking measures to eliminate the consequences of incidents		
IM.6	Planning and taking measures to prevent the recurrence of incidents		
Management of configuration of the information system and the personal data protection system (MC)			
MC.1	Determination of persons who are authorized to modify the information system configuration and the personal data protection system	At the level of: • the Platform's physical	At the level of the client's virtual infrastructure and Docker containers

Requirement source	Measures to ensure the security of personal data	The Yandex.Cloud Platform's integrated protection mechanisms	Protection measures to be taken by clients to ensure level 3 security
MC.2	Control of modification of the information system configuration and the personal data protection	hardware; • the system for controlling the virtualization environment; • Platform service/system servers and other virtual devices. • the Platform's software	
MC.3	Analysis of potential impact of planned modifications in the information system configuration and the personal data protection system on the protection of personal data and coordination of the modifications in the information system configuration with an officer (employee) in charge of personal data security		
MC.4	Documentation of information (data) about modifications in the information system configuration and the personal data protection system		