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. Л024-00107-00/00583151 dated November 22 2016, issued by Federal Service for Technical and Export Control (FSTEC), represented by

CEO Alexander Yurievich 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 BareMetal service 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
- Yandex DC Kaluga LLC, 1-y Avtomobilniy str, 8, Kaluga, 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 **Yandex BareMetal service** 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 BareMetal service** ensures: **level 1 personal data protection.**

Appendix 1 provides a short summary of integrated protection mechanisms on the **Yandex BareMetal service** and protection measures which enable clients to comply with the requirements of the laws of the Russian Federation for level 1 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 BareMetal service with the requirements of Federal Law No. 152 "On Personal Data" and regulations thereunder.

Signed on **October 13, 2025**

L.S. (Signature) CEO of CardSec LLC A. Yu. Ivanov
(Initials, last name)

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «Кард Секьюрити» ОГРН 5137746248138 * МОСКВА * «Card Security» Limited Liability Company *
ООО «Кард Сек»
«Card Sec» LLC

Appendix No. 1 Allocation of Responsibility for Personal Data Protection

Requirement source	Measures to ensure the security of personal data	The Yandex.Cloud Service'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	Not applicable: The specified requirement is fulfilled using the functionality of the certified Yandex.Cloud cloud computing environment, which has a certificate of conformity no. L024-00107-00/00580503.00099.2023	At the level of the deployed infrastructure, including OS, DBMS, software, virtualization tools and network security mechanisms
IA.2	Identification and authentication of devices, including stationary, mobile and portable devices		N/A
IA.3	Identity management including the creation, assignment and destruction of IDs		At the level of the deployed infrastructure, including OS, DBMS, software, virtualization tools and network security mechanisms
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)		
Management of access by access subjects to access objects (MA)			
MA.1	Management (creation, activation, blocking and destruction) of user accounts including external users	Not applicable: The specified requirement is fulfilled using the functionality of the certified Yandex.Cloud cloud computing environment, which has a certificate of conformity no. L024-00107-00/00580503.00099.2023	At the level of the deployed infrastructure, including OS, DBMS, software, virtualization tools and network security mechanisms
MA.2	Implementation of necessary access control methods (discretionary, mandate, role-based or other method), types (reading, recording, execution or other type) and rules		
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 Service's physical hardware; • the Service's service networks; • access restriction between network segments of the Service'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.

Requirement source	Measures to ensure the security of personal data	The Yandex.Cloud Service's integrated protection mechanisms	Protection measures to be taken by clients to ensure level 3 security
MA.4	Separation of powers (roles) of users, administrators and persons in charge of the information system's operation	Not applicable: The specified requirement is fulfilled using the functionality of the certified Yandex.Cloud cloud computing environment, which has a certificate of conformity no. L024-00107-00/00580503.00099.2023	At the level of the deployed infrastructure, including OS, DBMS, software, virtualization tools and network security mechanisms
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	Not applicable: The specified requirement is fulfilled using the functionality of the certified Yandex.Cloud cloud computing environment, which has a certificate of conformity no. L024-00107-00/00580503.00099.2023	At the level of the deployed infrastructure, including OS, DBMS, software, virtualization tools and network security mechanisms
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)	Not applicable: The specified requirement is fulfilled using the functionality of the certified Yandex.Cloud cloud computing environment, which has a certificate of conformity no. L024-00107-00/00580503.00099.2023	When organizing such interaction with the deployed infrastructure, including OS, DBMS, software, virtualization tools and network security mechanisms
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 .	Not applicable: The specified requirement is fulfilled using the functionality of the certified Yandex.Cloud cloud computing environment, which has a certificate of conformity no. L024-00107-00/00580503.00099.2023	At the level of the deployed infrastructure, including OS, DBMS, software, virtualization tools and network security mechanisms
SER.3	Restrictions for only authorized software and/or installation of its components.		
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 Service	N/A
PMM.2	Access management for machine media with personal data	At the level of physical data storage media used in the Service	N/A
PMM.8	Destruction (deletion) or depersonalization of personal data on machine-readable media when transferred between users or to external organizations for	At the level of physical data storage media used in the Service	N/A

Requirement source	Measures to ensure the security of personal data	The Yandex.Cloud Service's integrated protection mechanisms	Protection measures to be taken by clients to ensure level 3 security
	repair or disposal, as well as the control of destruction (deletion) or depersonalization		
Security event logging (SEL)			
SEL.1	Determining security events to be logged and their storage time	Not applicable: The specified requirement is fulfilled using the functionality of the certified Yandex.Cloud cloud computing environment, which has a certificate of conformity no. L024-00107-00/00580503.00099.2023	At the level of the deployed infrastructure, including OS, DBMS, software, virtualization tools and network security mechanisms
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 Company is responsible for ensuring the physical and network security of the Service and is not able to manage security measures at the client server level.	At the level of the deployed infrastructure, including OS, DBMS, software, virtualization tools and network security mechanisms
VP.2	Updating the database of malware (virus) signatures		
Intrusion detection system (IDS)			
IDS.1	Intrusion detection	At the level of: • physical Service hardware; • Service 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	Not applicable: The specified requirement is fulfilled using the functionality of the certified Yandex.Cloud cloud computing environment, which has a certificate of conformity no. L024-00107-00/00580503.00099.2023	At the level of the deployed infrastructure, including OS, DBMS, software, virtualization tools and network security mechanisms
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		
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	Not applicable: The specified requirement is fulfilled using the functionality of the certified Yandex.Cloud	At the level of the deployed infrastructure, including OS, DBMS, software, virtualization

Requirement source	Measures to ensure the security of personal data	The Yandex.Cloud Service's integrated protection mechanisms	Protection measures to be taken by clients to ensure level 3 security
		cloud computing environment, which has a certificate of conformity no. L024-00107-00/00580503.00099.2023	tools and network security mechanisms
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 Service 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 Service hardware; • Service service/system servers and other virtual devices.	At the level of the client's ISPDn, backup and recovery of personal data is performed by the client. At the OS level of the physical servers of the Service and the client's infrastructure, data is backed up by the client 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	Not applicable: The specified requirement is fulfilled using the functionality of the certified Yandex.Cloud cloud computing environment, which has a certificate of conformity no. L024-00107-00/00580503.00099.2023	At the level of the deployed infrastructure, including OS, DBMS, software, virtualization tools and network security mechanisms
VEP.2	Control of access by access subjects to access objects in virtual infrastructure including within virtual machines		
VEP.3	Virtual infrastructure security events logging		
VEP.6	Managing the movement of virtual machines (containers) and data processed on them		
VEP.7	Control of virtual infrastructure and its configuration integrity		
VEP.8	Data backup, backup of hardware and virtual infrastructure software, as well as communication channels within the virtual infrastructure		
VEP.9	Implementation and management of virus protection in virtual infrastructure	Not applicable: The specified requirement is fulfilled using the functionality of the certified Yandex.Cloud cloud computing environment, which has a certificate of conformity no. L024-00107-00/00580503.00099.2023	At the level of the deployed infrastructure, including OS, DBMS, software, virtualization tools and network security mechanisms
VEP.10	Segmentation of virtual infrastructure for processing of personal data by a user and/or a group of users		At the level of client's network segments
Protection of hardware (PH)			

Requirement source	Measures to ensure the security of personal data	The Yandex.Cloud Service's integrated protection mechanisms	Protection measures to be taken by clients to ensure level 3 security
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
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	Not applicable: The specified requirement is fulfilled using the functionality of the certified Yandex.Cloud cloud computing environment, which has a certificate of conformity no. L024-00107-00/00580503.00099.2023	At the level of the deployed infrastructure, including OS, DBMS, software, virtualization tools and network security mechanisms
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 deployed infrastructure, including OS, DBMS, software, virtualization tools and network security mechanisms
PIS.11	Authenticity of network connections (interaction sessions), including protection against spoofing of network devices and services		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 the deployed infrastructure, including OS, DBMS, software, virtualization tools and network security mechanisms
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.	Not applicable: The specified requirement is fulfilled using the functionality of the certified Yandex.Cloud cloud computing environment, which has a certificate of conformity no. L024-00107-00/00580503.00099.2023	From employees of client organization or its contractors
IM.2	Incident detection, identification and registration	Not applicable: The specified requirement is fulfilled using the functionality of the certified Yandex.Cloud cloud computing environment, which has a certificate of	At the level of the deployed infrastructure, including OS, DBMS, software, virtualization tools and network security mechanisms

Requirement source	Measures to ensure the security of personal data	The Yandex.Cloud Service's integrated protection mechanisms	Protection measures to be taken by clients to ensure level 3 security
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	conformity no. L024-00107-00/00580503.00099.2023	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 deployed infrastructure, including OS, DBMS, software, virtualization tools and network security mechanisms
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 Service's physical hardware; • Service service/system servers and other virtual devices. • the Service's software	At the level of the deployed infrastructure, including OS, DBMS, software, virtualization tools and network security mechanisms
MC.2	Control of modification of the information system configuration and the personal data protection		
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		