Card Security

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

Card Security LLC

(Name of a manufacturer, first name, patronymic and last name of an individual entrepreneur that accepted the declaration of compliance) (address, telephone, fax)

License for technical protection of confidential information No. L024-00107-00/00583151 dated November 22, 2016 issued by Federal Service for Technical and Export Control (FSTEC)

represented by **CEO Alexander Yuryevich Ivanov**

(first name, patronymic and last name of CEO of an entity on behalf whereof the declaration is accepted)

states that **it audited the "Data Residency-as-a-Service Platform" Personal Data Information System (PDIS) for the Services specified in Appendix 1**

(name, type and model of products covered by the declaration, code OK 005-93 and/or Commodity Nomenclature for Foreign Economic Activities of CIS)

and the infrastructure they are based on consisting of hardware and software. Hardware are located in the data centers of the service provider Yandex.Cloud LLC.

Following the results of threat modelling, performed in the form of a risk assessment, the third type threats were recognized relevant, while the first type and second type threats were recognized irrelevant. According to the compliance audit, all the necessary measures were taken to neutralize the relevant personal data threats.

The above mentioned PDIS was 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 "Data Residency-as-a-Service Platform" PDIS ensures: **the 1st level of personal data security.**

Appendix 2 provides a short summary of integrated protection mechanisms on the "Data Residency-as-a-Service Platform" PDIS and protection measures to comply with the requirements of the laws of the Russian Federation for the first level of personal data security.

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

InCountry, INC has adopted the organizational and technical measures ensuring the compliance of the "Data Residency-as-a-Service Platform" PDIS with the requirements of Federal Law No. 152 "On Personal Data" and regulations thereunder.

Signed on **June 23 , 2023**

L.S.

(Signature)

CEO of CardSec LLC Alexander Ivanov

(Initials, last name)

Card Security

Appendix No. 1 Services in the "Data Residency-as-a-Service Platform" PDIS audit scope

1. REST API and Software Development Kit (SDK)
2. Border
3. Data Residency for Salesforce

Card Security

Appendix No. 2 Assessment of requirements of Federal Law 152 implementation

Requirement source	Measures to ensure the security of personal data	Protection measures that are implemented to ensure the first security level
Identification and authentication of access subjects and access objects (IA)		
IA.1	Identification and authentication of users who are the operator's employees	Identification and authentication of users in the Platform is carried out using a login/password pair. Authentication is reinforced by using MFA. Access control measures are implemented by the service-provider Yandex.Cloud LLC on hardware and virtualization environment level.
IA.2	Identification and authentication of devices, including stationary, mobile and portable devices	At the level of the Platform's physical hardware are implemented by the service-provider Yandex.Cloud LLC
IA.3	Identity management including the creation, assignment and deletion of IDs	Access control procedures are documented in «InCountry Identity & Access Management Standard». All users are granted access only after approval by the authorized personnel. All users are assigned unique user IDs. Accounts that are no longer used are disabled or removed. Access control mechanisms of operation systems and software are in use. Access control measures are implemented by the service-provider Yandex.Cloud LLC on hardware and virtualization environment level.
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	Procedures for managing users' credentials are documented in «InCountry Identity & Access Management Standard» and «InCountry Password Protection Standard». All users' credentials are securely stored. Compromised users' credentials are changed immediately. Access control mechanisms of operation systems and software are in use. Access control measures are implemented by the service-provider Yandex.Cloud LLC on hardware and virtualization environment level.
IA.5	Feedback protection during the input of authentication information	All input of authentication information, such as passwords, is masked. Access control mechanisms of operation systems and software are in use. Access control measures are implemented by the service-provider Yandex.Cloud LLC on hardware and virtualization environment level.
IA.6	Identification and authentication of users who are not the operator's employees (external users)	Identification and authentication of external users in the Platform is carried out using a login/password pair. Authentication is reinforced by using MFA. Access control mechanisms of operation systems and software are in use.
Management of access by access subjects to access objects (MA)		
MA.1	Management (creation, activation, blocking and deletion) of user accounts including external users	Access control procedures are documented in «InCountry Identity & Access Management Standard». All users are granted access after a confirmation by authorized personnel only. All users are given access to systems and information on a need-to-know basis and access is canceled when no longer needed. Access control mechanisms of operation systems and software are in use. Access control measures are implemented by the service-provider Yandex.Cloud LLC on hardware and virtualization environment level.

Requirement source	Measures to ensure the security of personal data	Protection measures that are implemented to ensure the first security level
MA.2	Implementation of necessary access control methods (discretionary, mandate, role-based or other method), types (reading, recording, execution or other type) and rules	Access control procedures are documented in «InCountry Identity & Access Management Standard». Role-based access control is used. Access control mechanisms of operation systems and software are in use. Access control measures are implemented by the service-provider Yandex.Cloud LLC on hardware and virtualization environment level.
MA.3	Management (filtration, routing, connection control, one-way transmission and other management methods) of information flows between devices, segments of the information system and information systems	Network flows are controlled by ACLs on network equipment. WAF is implemented.
MA.4	Allocation of powers (roles) of users, administrators and persons in charge of the information system's operation	Access control procedures are documented in «InCountry Identity & Access Management Standard». Development and production operation functions are separated. Access control mechanisms of operation systems and software are in use. Access control measures are implemented by the service-provider Yandex.Cloud LLC on hardware and virtualization environment level.
MA.5	Granting minimum necessary rights and privileges to users, administrators and persons in charge of the information system's operation	Access control procedures are documented in «InCountry Identity & Access Management Standard». All users are granted minimum necessary rights to systems for performing their duties. Access control mechanisms of operation systems and software are in use. Access control measures are implemented by the service-provider Yandex.Cloud LLC on hardware and virtualization environment level.
MA.6	Limiting unsuccessful information system login attempts (access to the information system)	Access control procedures are documented in «InCountry Identity & Access Management Standard». User accounts are blocked after 5 unsuccessful login attempts. Access control mechanisms of operation systems and software are in use. Access control measures are implemented by the service-provider Yandex.Cloud LLC on hardware and virtualization environment level.
MA.10	Blocking information system access session upon the expiry of a determined user idle (inactivity) time or at the user's request	Access control procedures are documented in «InCountry Identity & Access Management Standard». User sessions are terminated after a set time of inactivity or after user request. Access control mechanisms of operation systems and software are in use. Access control measures are implemented by the service-provider Yandex.Cloud LLC on hardware and virtualization environment level.
MA.11	Authorization (ban) of user's acts permitted before identification and authentication	Authentication is required for any users' actions within corporate systems. Access control measures are implemented by the service-provider Yandex.Cloud LLC on hardware and virtualization environment level.

MA.13	Implementation of protected remote access by access subjects to access objects through external information telecommunication networks	User remote access to the Platform through communication channels is performed by using special tools.
MA.14	Regulation and control of usage of wireless access technologies in the information system	The use of wireless device is controlled and regulated by the «InCountry Corporate Device Security Standard» and «InCountry Acceptable Use Policy».
MA.15	Regulation and control of usage of mobile equipment in the information system	The use of mobile devices is controlled and regulated by the «InCountry Corporate Device Security Standard» and «InCountry BYOD Policy»
MA.16	Management of interaction with information systems of external organizations (external information systems)	User interaction with information systems of external organizations is regulated. Only approved external systems can be used to process or store non-public corporate data. There are contracts with the service provider Yandex.Cloud LLC.
MA.17	Providing trusted loading of computer equipment	At the level of the Platform's physical hardware is implemented by the service-provider Yandex.Cloud LLC.
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 .	Approval of installed packages during software updates. It is not possible to install any package version as a part of the release, except for agreed. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
SER.3	Restrictions for only authorized software and/or installation of its components.	
Protection of machine-readable media containing personal data (PMM)		
PMM.1	Accounting for machine media with personal data	Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
PMM.2	Access management for machine media with personal data	Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
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	Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
Security event logging (SEL)		
SEL.1	Determination of security events to be logged and their storage time	Logging requirements are documented in «InCountry Logging and Monitoring Standard». Security event logging is configured for all systems in the production environment. SIEM is used. Audit logging is implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
SEL.2	Determination of scope and contents of information about security events	Logging requirements are documented in «InCountry Logging and Monitoring Standard». All security event logs contain information such as time, user ID and description of the event. Audit logging is implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.

SEL.3	Collection, recording and storage of security events information during the determined storage time	Logging requirements are documented in «InCountry Logging and Monitoring Standard». All security events are stored according to the «InCountry Deletion and Retention Policy». SIEM is used. Audit logging is implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
SEL.5	Monitoring (viewing, analyzing) the results of registering security events and responding to them	SIEM is used. Audit logging is implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
SEL.7	Protection of security events information	All security events are protected from unauthorized access and modification. Audit logging is implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
Virus protection (VP)		
VP.1	Implementation of virus protection	Antivirus protection is implemented. Anti-malware protection is implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
VP.2	Updating the database of malware (virus) signatures	Antivirus protection is implemented. Antivirus databases are updated on a daily basis. Anti-malware protection is implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
Intrusion detection system (IDS)		
IDS.1	Intrusion detection	HIDS is used. IDS are implemented by the service-provider Yandex.Cloud LLC on hardware and virtualization environment level.
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	Internal and external vulnerability scanning is performed on a regular basis and before major changes in production systems. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
AS.2	Control of software updates installation including software updates of information protection means	«InCountry Change Management Standard» is documented. Internal and external vulnerability scanning is performed on a regular basis and after major changes in production systems. All changes to production systems pass through a formal change management process which includes testing. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
AS.3	Control of operability, settings and faultless operation of software and information protection means	«InCountry Change Management Standard» is documented. All changes to production systems pass through a formal change management process which includes testing. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
AS.4	Control of composition of hardware, software and information protection means	«InCountry Change Management Standard» is documented. Only approved software is installed in production systems. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.

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	Password policies are implemented. Information security audit are in place. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
Integrity of the information system and personal data (INT)		
INT.1	Software integrity control, including information security software	Integrity monitoring tools are implemented on the Platform's virtual servers. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
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.
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	Automated monitoring of the Platform's performance is in place. Backups are performed, the data is restored from backups if necessary. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
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	All staff having access to customer data (including administrators) are authenticated using MFA. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
VEP.2	Control of access by access subjects to access objects in virtual infrastructure including in virtual machines	All users are given access to systems and information on a need-to-know basis and access is revoked when is no longer needed. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
VEP.3	Virtual infrastructure security events logging	Security event logging is configured for all systems in the production environment. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
VEP.6	Managing the movement of virtual machines (containers) and data processed on them	Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
VEP.7	Control of virtual infrastructure and its configuration integrity	Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
VEP.8	Data backup, backup of hardware and virtual infrastructure software, as well as communication channels within the virtual infrastructure	Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.

VEP.9	Implementation and management of virus protection in virtual infrastructure	Antivirus protection is implemented for production systems. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
VEP.10	Segmentation of virtual infrastructure for processing of personal data by a user and/or a group of users	Each customer has a dedicated segregated space for storing his data (e.g. a separate server or a DB instance). Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
Protection of hardware (PH)		
PH.3	Control and management of physical access to hardware, information protection means, operation support equipment and to 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	Responsibility of the subcontracted service-provider Yandex.Cloud LLC.
PH.4	Location of information output (display) devices preventing unauthorized viewing thereof	Responsibility of the subcontracted service-provider Yandex.Cloud LLC.
PH.5	Protection against the external impacts (environmental impacts, interruptions of power supply, air conditioning and other external factors)	Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
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	Users of the Platform do not have administrative privileges. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
PIS.3	Protection of personal data against disclosure, modification and forcing (input of false information) during transmission (preparation for transmission) thereof through communication channels which go beyond the controlled zone including wireless communication channels	User remote access to the Platform through communication channels is performed by using special tools. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
PIS.11	Authenticity of network connections (interaction sessions), including protection against spoofing of network devices and services	User remote access to the Platform through communication channels is performed by using special tools. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
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	Users of the Platform do not have administrative privileges. Integrity monitoring tools are implemented on the Platform's virtual servers. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
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	Firewalls are used within the internal network. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
PIS.20	Protection of wireless environment	Usage of wireless device is controlled and regulated by the «InCountry Corporate Device Security Standard».

Identifying and responding to incident (IM)		
IM.1	Identification of persons responsible for identifying and responding to incidents.	Information security incidents are managed in accordance with the following documents: «InCountry Data Breach Notification Policy», «InCountry Security Incident Classification Matrix», «InCountry Security Incident Communication Plan», «InCountry Security Incident Response Plan». Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
IM.2	Incident detection, identification and registration	
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	
IM.4	Incident analysis, including identification of sources and causes of incidents, as well as assessment of their consequences	
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 that are authorized to modify the information system configuration and the personal data protection system	Change management is documented in «InCountry Change Management Standard». Only Operations Team is authorized to make changes to production systems. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
MC.2	Control of modification of the information system configuration and the personal data protection system	Change management is documented in «InCountry Change Management Standard». Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
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	Change management is documented in «InCountry Change Management Standard». All changes to production systems pass through a formal change management process which includes testing. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.
MC.4	Documentation of information (data) about modifications in the information system configuration and the personal data protection system	Change management is documented in «InCountry Change Management Standard». All changes to production systems pass are consistent with a formal change management process which includes testing. Control measures are implemented by the service-provider Yandex.Cloud LLC on the level of virtualization environment.