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 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. 3099 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 personal data protection system of InCountry's data residency-as-a-service platform**

(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 service providers Yandex.Cloud LLC and Selectel LLC.

Following the results of threat modelling, performed in the form of risk assessment, the third type threats were recognized relevant, while the first type and second type threats were recognized 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 above PDIS ensures: **the 3rd level of personal data security.**

Appendix 1 provides a short summary of integrated protection mechanisms and protection measures to comply with the requirements of the laws of the Russian Federation for the third personal data security level.

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

InCountry, INC has adopted the organizational and technical measures ensuring the compliance of InCountry's data residency-as-a-service platform PDIS with the requirements of Federal Law No. 152 "On Personal Data" and regulations thereunder.

Signed on **September 8, 2020**

L.S.

(Signature)

CEO of CardSec LLC Alexander Ivanov

(Initials, last name)

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ * ОГРН 5137746246138 * МОСКВА *
«Кард Секьюрити»
«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	Protection measures that are implemented to ensure the third 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	The Google MFA is implemented in Data-Residency-as-a-Service. Access control measures are implemented by service-providers Yandex.Cloud LLC and Selectel LLC on hardware and virtualization environment level.
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. Users that no longer require access are disabled or removed. Access control mechanisms of operation systems and software are in use. Access control measures are implemented by service-providers Yandex.Cloud LLC and Selectel 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 manage 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 service-providers Yandex.Cloud LLC and Selectel 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 service-providers Yandex.Cloud LLC and Selectel LLC on hardware and virtualization environment level.
IA.6	Identification and authentication of users who are not the operator's employees (external users)	The Google MFA is implemented in Data-Residency-as-a-Service. Access control mechanisms of operation systems and software are in use. All external users, such as contractors or consultants, are authenticated before getting access to corporate systems.
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.

Requirement source	Measures to ensure the security of personal data	Protection measures that are implemented to ensure the third security level
		All users are given access to systems and information on a need-to-know basis and access is revoked when no longer needed. Access control mechanisms of operation systems and software are in use. Access control measures are implemented by service-providers Yandex.Cloud LLC and Selectel LLC on hardware and virtualization environment 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 service-providers Yandex.Cloud LLC and Selectel 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.
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 service-providers Yandex.Cloud LLC and Selectel 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 service-providers Yandex.Cloud LLC and Selectel 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». Users are assigned roles with minimum privileges. The number of unsuccessful login attempts is limited. Access control mechanisms of operation systems and software are in use. Access control measures are implemented by service-providers Yandex.Cloud LLC and Selectel 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». Users are assigned roles with minimum privileges. User sessions are terminated after a set time of inactivity. Access control mechanisms of operation systems and software

Requirement source	Measures to ensure the security of personal data	Protection measures that are implemented to ensure the third security level
		are in use. Access control measures are implemented by service-providers Yandex.Cloud LLC and Selectel LLC on hardware and virtualization environment level.
MA.11	Authorization (ban) of user's acts permitted before identification and authentication	Authentication required for any users' actions within corporate systems. Access control measures are implemented by service-providers Yandex.Cloud LLC and Selectel 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	All external communication channels are encrypted.
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 Wireless Standard.
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 Mobile Device Standard.
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 service providers Yandex.Cloud LLC and Selectel LLC.
Protection of machine-readable media containing personal data (PMM)		
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	All media containing non-public corporate data, such as laptop drives, is encrypted. Control measures are implemented by service-providers Yandex.Cloud LLC and Selectel 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 «Logging and Monitoring Standard». Security event logging is configured for all systems in the production environment. SIEM Opsgenie is used. Audit logging is implemented by service-providers Yandex.Cloud LLC and Selectel LLC on the level of virtualization environment.
SEL.2	Determination of scope and contents of information about security events	Logging requirements are documented in «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 service-providers Yandex.Cloud LLC and Selectel 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 «Logging and Monitoring Standard». All security events are stored according to the Deletion and Retention Policy. SIEM Opsgenie is used. Audit logging is implemented by service-providers

Requirement source	Measures to ensure the security of personal data	Protection measures that are implemented to ensure the third security level
		Yandex.Cloud LLC and Selectel 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 service-providers Yandex.Cloud LLC and Selectel 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 service-providers Yandex.Cloud LLC and Selectel 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 service-providers Yandex.Cloud LLC and Selectel LLC on the level of virtualization environment.
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 service-providers Yandex.Cloud LLC and Selectel 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 service-providers Yandex.Cloud LLC and Selectel 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 service-providers Yandex.Cloud LLC and Selectel 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 service-providers Yandex.Cloud LLC and Selectel LLC on the level of virtualization environment.
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 service-providers Yandex.Cloud LLC and Selectel 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.

Requirement source	Measures to ensure the security of personal data	Protection measures that are implemented to ensure the third security level
		Control measures are implemented by service-providers Yandex.Cloud LLC and Selectel 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 service-providers Yandex.Cloud LLC and Selectel 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 service-providers Yandex.Cloud LLC and Selectel 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 service-providers Yandex.Cloud LLC and Selectel 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-providers (Yandex.Cloud LLC and Selectel LLC).
PH.4	Location of information output (display) devices preventing unauthorized viewing thereof	Responsibility of the subcontracted service-providers (Yandex.Cloud LLC and Selectel LLC).
Protection of the information system, its equipment, communication and data transmission systems (PIS)		
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	All external communication channels are encrypted.
PIS.20	Protection of wireless environment	Usage of wireless device is controlled and regulated by the Wireless Standard.
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 service-providers Yandex.Cloud LLC and Selectel 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 service-providers Yandex.Cloud LLC and Selectel LLC on the level of virtualization environment.
MC.3	Analysis of potential impact of planned modifications in the information system	Change management is documented in «InCountry Change

Requirement source	Measures to ensure the security of personal data	Protection measures that are implemented to ensure the third security level
	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	Management Standard». All changes to production systems pass through a formal change management process which includes testing. Control measures are implemented by service-providers Yandex.Cloud LLC and Selectel 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 service-providers Yandex.Cloud LLC and Selectel LLC on the level of virtualization environment.