**Information material for open consultation on "Building an enabling environment for access to the Internet" within the frameworks of CWG-Internet**

**(13-14 October 2016, Geneva, Switzerland)**

**Mobile TeleSystems PJSC**

Further development of the civilization goes hand-in-hand with provisioning to its citizens an access to information as freely as possible, *inter alia*, through the Internet. At the same time, the right for free access to information for a certain individual shall not be detrimental to interests and civil liberties of other citizens. Practical implementation of this principle imposes duty upon communication operators/providers to develop an effective and viable mechanism, a set of administrative, organizational, legal and special engineering measures for protection of personal information and other confidential information of all subjects which are directly or indirectly involved into the information exchange.

For the purpose to meet requirements of Articles 53 and 63 of [Federal Law "On Communication"](http://minsvyaz.ru/ru/documents/3068/) by operators to ensure confidentiality of data on subscribers, services provided and to ensure secrecy of communication, MTS PJSC has been implementing the organizational, legal and engineering measures to protect the above information from an unauthorized access to and dissemination of, such information.

MTS PJSC has enacted the following in-house legal acts which are mandatory for all personnel authorized for operations with confidential information and secrecy of communication:

* PT-010 Policy "Personal data handling in Mobile TeleSystems PJSC";
* PT-046 Policy "Personal data security in PJSC MTS";
* PT-002 Policy "Regulations on the information security (confidentiality) mode in MTS PJSC";
* RP-140 Process Regulations "Paperwork management for physical storage media with information constituting a trade secret and other confidential information of MTS PJSC";
* ST-053-5 Standard "Requirements for physical security management at the MTS PJSC premises";
* PT-062 Policy "Requirements for information security in PJSC MTS" and other in-house legal acts on security of subscribers’ data and secrecy of communication.

According to the in-house legal acts, requirements of Sarbanes-Oxley Act in corporate governance and internal control, national legislation and international standards in information security management, the following measures are implemented amongst others:

* Pass and site access control procedures, internal security regime for premises accommodating information systems for the pass control and 24-hour security checkpoints in the buildings of MTS PJSC;
* Restriction of user rights, distributed user access to information and user logging;
* Application of information encryption tools, network firewalls and other mechanisms for information protection which are successfully tested for conformity assessment;
* Access to secrecy of communication is possible exclusively for the operator’s managers (employees), respecting conditions and requirements of the Russian Law.

Security of users’ personal data when they are processed in MTS PJSC information system for personal data (ISPD) is ensured by centralized system for protection of personal data (SPPD) integrated into infrastructure of information security of corporate information system (CIS).

The SPPD includes organizational and technical measures, which are implemented through security mode of confidential information and by introduction of technical facilities for information protection. Arrangement of works to create SPPD and application of centralized facilities for information protection are executed by structural security subdivision.

For the purpose to improve the system for protection of personal data and minimize possible risks for infringement of legislation on personal data by security subdivisions, Corporate Centre of MTS Group permanently implements additional measures to improve personal data protection:

* Gathering and recording information on processed personal data, automated and non-automated processes of personal data handling, information resources used for personal data processing (circulation of paper documents, corporate information system, application information systems, databases, Internet services and etc.)
* Development of list for personal data processed in MTS PJSC, identification of targets, reasons for processing and terms of personal data storage
* Distribution of responsibility for tasks/functions on processing and security of personal data between structural subdivisions of MTS PJSC
* Review/development of corporate local normative acts regulating data processing in accordance with requirements of the Russian Federation legislation, taking into account international law and best practices
* Synchronization of measures to provide security of personal data in MTS Group
* Assessment of fulfillment for legislation requirements on personal data when implementing various business cases by commercial subdivisions of MTS PJSC
* Optimization (re-engineering) of business processes with personal data processing for the purpose to minimize regulatory risks
* Unification of organizational solutions on processing and protection of personal data in MTS Group.

Monitoring the above measures is assigned to specialized subdivisions of the Company, responsible for implementing the centralized system for protection of confidential information and secret of communication, integrated into the infrastructure of the corporate information system.

MTS PJSC also applies the following measures to protect subscribers’ information:

* Centre for operative network monitoring (CONM) is deployed to detect and block cyber-attacks. A process to establish interaction between CONM and State system for cyber-attack detection, prevention and elimination of consequences (GosSOPKA) is going on
* A system for antivirus protection of subscribers is deployed, which warns subscribers about possible virus infection of the subscriber device and recommends to apply antivirus measures
* Services to protect subscribers from DDoS attacks are offered
* Antispam system against SMS distribution is deployed, which allows protecting subscribers from unwanted messages and fraud
* Services for cryptographic protection of information in communication channels are provided
* Parental Control service is provided for to protect children online
* Protection of user devices from unauthorized access and use is implemented (botnets).

**Summary:**

There are still organizational and legal challenges associated with the lack of harmonized position between participants of the international interchange of information on application of uniform standards for information security, caused by the difference in national laws.

Main areas where the efforts to protect Internet users and Internet-service users face challenges in transboundary information environment are the following:

* Standardization of technical measures protecting information in the "Internet of Things"
* Standardization of technical measures protecting personal data during cross-border processing
* Standardization of cryptographic algorithms for cross-border information protection during cross-border interaction, and to provide legally valid circulation of electronic documents
* Interaction of national and commercial Centers for monitoring information security to counteract hacker attacks and cybercrime in the Internet
* Standardization of processing and protection of Big Data.