



## **OPEN CONSULTATION ON THE DEVELOPMENTAL ASPECTS OF THE INTERNET**

**(February, 03 2017, Geneva, Switzerland)**

### **Russian experience of regulation processing (usage) of the personal data as a one of the key elements for personal digital authentication**

#### **1. Summary**

- Russian Federation has developed and implemented public policy for personal data processing as well as many other countries.
- Nevertheless, public policies related to identification and authentication systems and processing of personal data are at different stages of development in various countries.
- One of the key issues is the cross-border transfer of personal data for global Internet services, where personal data is transmitted and can be processed on servers outside the legal framework of the country of origin.
- There is a strong need of all stakeholders to share knowledge and discuss issues related to personal data protection.
- CWG-Internet can initiate and conduct such discussion regarding public policies for identification and authentication issues in general and personal data processing in particular for benefits of all stakeholders.

#### **2. Introduction**

During previous session in October, 2016 CWG-Internet decided to hold an open consultation, online and physical, on the following topic – «Developmental Aspects of the Internet », including following questions:

1. What are the developmental aspects of the Internet (for example, economic, social, regulatory and technical aspects), especially for developing countries?

2. How can governments and other stakeholders promote the developmental aspects of the Internet?

3. What are the challenges and opportunities?

At the same meeting, the Russian Federation has taken the initiative, which was supported by number of Member States to organize a discussion on key aspects of personal electronic authentication.

In respect that personal authentication is one of the key elements of modern Internet services and basis for development digital economy we represent material related to this subject in the framework of public consultation by CWG-Internet.

Developmental aspects of the Internet imply the entire system of organizational and/or technical actions, the set of which is defined by the level and the range of services offered online. If we are considering «core» Internet services, then «developmental aspects» means first of all connectivity and building physical infrastructure for access. Advanced e2e online services require both access and secure environment for work through the Internet. In this case «developmental aspects» will further include capabilities for protection from malicious activity, fraudulence, viruses, spam, capabilities for secure and confidential Internet operations, including regulatory frameworks and legislative initiatives for protection of private life and network stability. Governments are the key guarantors of rights and obligations in the Internet. In this way personal authentication practice and regulation are mandatory aspects for Internet development.

Necessary to highlight that personal authentication first of all is based on processing and management of personal data. We prepared information regarding Russian experience in regulation of personal data as a basis for future discussion.

### **3. Russian experience of personal data protection**

Russian Federation has adopted the Federal Law [FZ-152 «On Personal Data»](#) July 27, 2006. This federal law was developed as a result of the ratification «Convention for the protection of individuals with regard to automatic processing

of personal data» (Council of Europe, CETS 108) by Russia. This law was intended to define requirements for personal data protection, which have been established in this Convention.

Now in Russia there are two laws in effect related to processing (usage) of the personal data:

- Federal Law [FZ-152 «On Personal Data»](#)
- Federal Law [FZ-242 «On Amendments to Certain Legislative Acts of the Russian Federation to clarify the processing of personal data order information and telecommunications networks»](#).

The main objective of this regulation is to protect the rights and freedoms of citizens in the processing of their personal data, including cross-border transfer.

Laws govern the relationship between private and public companies and organizations (operators of personal data) that transmit or process personal data and individuals (subjects of personal data).

Since its first publication in 2006 the Federal Law [FZ-152 «On Personal Data»](#) has been significantly changed, and now personal data are required to be stored in the territory of the Russian Federation and be protected according with defined rules. In practice, this leads to an increase in the business responsibility for data processing.

Under term «information system» law defines «a set of personal data contained in the database, as well as information technology and the technical tools to carry out processing of personal data using automated tools or without the use of such tools». Under «personal data» (PD) in the law refers to any information which relates directly or indirectly «to a specific individual or identified on the basis of such information individual» (subject of personal data, PD subject).

The first type of data - the actual data of the client. For example, it is a name, date and place of birth, passport number, and for legal entities - company data. At the beginning of the work client approves transformation of PD to the company, and a company accepts requirements of federal laws for working with PD. The second type of data is the client's information that is actually stored directly

on the servers. This information just a more meaningful and important object of protection. Examples of such data might be the login password for internet services and client's preferences, email, personal financial data from clients at the banking server. For legal entities (companies) range of such information more widely - customer databases, accounting and specialized software.

Legal entities are responsible for the protection of this information according to federal law.

The law introduces the concept and term of "personal data operator" (PD operator). "Operator" in the term in the law, referred to any person or organizations who deal with other individuals' (subject of personal data) personal data processing. Russian Federation established a register of operators engaged in processing of personal data. Currently, the register contains information on 369 136 personal data operators.

Article 22 of the Federal Law «On Personal Data» define duty of PD operators who processing personal data to notify the authorized body for the protection of personal data of its intention to work with personal data as soon as they start such activity. According to this article, PD operators have to fulfill a number of obligations to protect PD in their information systems, for example:

- Send notification from PD operator to the authorized body;
- Get a written consent from the subjects of PD for processing its data;
- Notify the subject of personal data regarding termination of the processing and the destruction of PD.

PD operator must obtain the consent of the PD subjects. The consent for personal data processing from PD subject (ie, the person to whom these data relate) can be written or verbal. Written approval must be obtained in certain cases, as:

- for inclusion PD in any public available list (Art. 8.);
- for processing of special categories of personal data, such as racial origin, political opinions and similar information (Art. 10);
- for processing of biometric PD (Art. 11);

- for data transfer abroad (Art. 12);
- for making of any decisions affecting rights and freedoms of PD subject in process of personal data automatic processing (Art. 16).

In addition, the law can define other cases. Moreover, the law (Art. 9) defines additional requirements for such written consent: consent must contain a handwritten or electronic signature of a person who gives it. Therefore, for such approval PD operators can't use normal procedure for written agreements/contracts established by the Civil Code, when the terms of the contract set out in separate document and the consent may be expressed by committing some action of PD subject.

Separately regulated PD subject rights for access to personal data, as well as the procedure for appealing against the actions or omissions of the PD operator.

The laws and regulations for processing and usage of the personal data in the Russian Federation are comprehensive and sufficient for lawful usage of the personal data of citizens, because according to the applicable law there is administrative responsibility for acts violations. Control for proper laws performance is obligated to the authorized executive body which is responsible for the protection of personal data – Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor). Roskomnadzor has rights to:

- request and obtain free of charge the relevant information required from businesses and individuals;
- carry out inspections on their own or with the assistance of other bodies;
- require from operator to perform actions prescribed by the applicable law;
- take actions to suspend or terminate the processing of personal data;
- address the court with claims for the rights of an indeterminate number of persons;

- submit an application to the regulatory authority of the operator of the suspension or revocation of operator license;
- refer to the law enforcement bodies materials for criminal cases;
- make proposals to the Government;
- involve the perpetrators to administrative responsibility.

Federal law does not only determine the personal data protection necessity, but also offers special methods to protect personal data.

[Order №21](#) (dated 18 February 2013) of the Federal Service for Technical and Export Control “On approval of the list and content of organizational and technical measures to ensure the security of personal data at its processing in information systems of personal data” defines scope of concrete actions for PD protection.

Measures to ensure the security of personal data are taken to protect personal data against unauthorized or accidental access, destruction, modification, blocking, copying, provision, distribution of personal data, as well as other illegal actions in relation to personal data.

Measures to ensure the security of personal data carried out under the personal data protection system include:

- identification and authentication of PD subjects to access facilities;
- access control and management for PD subjects;
- limitation of the software environment;
- protection of computer memory & records media on which personal data are stored and/or processed ;
- check and log the security events;
- anti-virus protection;
- detection (prevention) intrusions;
- monitoring (analysis) of personal data protection;
- ensuring the integrity of information systems and personal data;
- ensuring the availability of personal data;
- protection of virtualization environments;

- protection of technical tools and facilities;
- protection of the information system, its resources, communications and data transmission systems;
- identification of incidents (one event or group of events) that can cause a malfunction or disruption of the functioning of the information system and (or) to the emergence of threats to the security of personal and response;
- configuration management of information systems and personal data protection system.

The list and content of measures to ensure the security of personal data necessary for each level of personal data protection are given in the Annex to this Order.

Thus, the stages of the information protection are defined, and can be listed as: definition of threats, development of security measures and control of records media, assessment of security measures and its effectiveness, monitoring of the entire security system. This approach allows operators to organize a reliable and efficient processing of PD operators.

Federal Law FZ-242 amends FZ-152 “On Personal Data”. In the old edition of the Law it provided foreign companies an advantage over Russian companies, because foreign companies could collect and process personal data of Russian citizens without fulfilment of law’ requirements. When FZ-242 took effect, foreign companies which work at Russian market or process PD of Russian citizens are required to locate personal data in Russia and moreover to be comply with Russian requirements for storing and usage of personal data. Examples of such companies are:

- Legal entities of foreign companies in the Russian Federation;
- Foreign companies which collect and process personal data via website without establishing a legal entity in the Russian Federation;

- Russian companies, which use foreign hosting providers, data-centers and cloud platforms.

Websites of foreign companies which do not follow the laws FZ-152 and FZ-242 can be blocked in the Russian Federation.

There are three ways to comply with the law of personal data localization:

- Fully relocate all personal data bases to Russia;
- Anonymize personal data and transfer it abroad;
- Transborder data transfer with saving of initial actual base in the territory of Russia.

In addition, the PD operator must ensure that foreign state addressed the transfer of personal data provide adequate protection of personal data of Russian citizens before the start of the cross-border transfer of personal data.

#### **4. Conclusion**

Thus, Russian Federation has developed and implemented public policies for personal data processing as well as in many other countries. These policies are aimed for secure operation of the personal data system which is a mandatory element of electronic identification and authentication systems.

Russian regulation is developed in line with European requirements stated in «Convention for the protection of individuals with regard to automatic processing of personal data» (Council of Europe, CETS 108).

Now in Russia there are two laws in effect related to processing (usage) of the personal data:

- Federal Law [FZ-152 «On Personal Data»](#)
- Federal Law [FZ-242 «On Amendments to Certain Legislative Acts of the Russian Federation to clarify the processing of personal data order information and telecommunications networks».](#)

Control for proper laws performance is obligated to the authorized executive body which is responsible for the protection of personal data – Federal Service for



Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor).

Finally, Russian Federation implemented systematic, integral approach for personal data processing with clear definitions of roles and responsibilities of all parties.