PERMANENT MISSION OF THE REPUBLIC OF MOLDOVA
TO THE UNITED NATIONS OFFICE IN GENEVA

No. 494/ R-ONU- 173

The Permanent Mission of the Republic of Moldova to the United Nations Office and other International Organizations in Geneva presents its compliments to the Office of the High Commissioner for Human Rights, Special Procedure Branch, an has the honour to submit herewith the contribution of the Republic of Moldova for the questionnaire of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, pursuant to Human Rights Council resolution 25/2.

The Permanent Mission of the Republic of Moldova to the United Nations Office and other International Organizations in Geneva avails itself of this opportunity to renew to the Office of the High Commissioner for Human Rights, Special Procedure Branch, the assurances of its highest consideration.

Geneva, 4 March 2015

Encl.: 5 pages

OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS
SPECIAL PROCEDURES BRANCH
Geneva

OHCHR REGISTRY

11 MARS 2015

Recipients : SPD

Enclosure

Courtesy translation

Freedom of individuals to express themselves online (Resolution 25/2 of the Human Rights Council)

As related to the request of Mr. David Kaye, special Rapporteur on the promotion of the right to freedom of opinion and expression, and in the view of the forthcoming report to the Human Rights Council, the Government of Republic of Moldova provides the following information.

Freedom of expression:

1) the ability of individuals and organizations to employ encryption tools in order to secure their transactions and communications online, and
2) the ability of individuals and organizations to employ tools to transact and communicate anonymously on line, are stated in the domestic laws protecting the privacy of correspondence and the freedom of opinion and expression, designed in accordance with the international and regional human rights laws as:
- The Universal Declaration of Human Rights (article 19);
- The International Covenant on Civil and Political rights (article 19);
- The European Convention on Human Rights (article 10).

It is important to mention that the main domestic law in this domain is the Constitution of the Republic of Moldova (article 32) followed by the Law no. 64 of 23 April 2010 on freedom of expression.

According to article 30 and 32 of the Constitution of the Republic of Moldova, *„every citizen shall be guaranteed the freedom of thought and opinion, as well as the freedom of expression in public way of word, image or any other means possible"* and *„The State shall ensure the privacy of letters, telegrams and other postal dispatches, as well as of telephone calls and other legal means of communication"*. The same provisions are stated in the article 3 of the Law on freedom of expression. It is necessary to specify that „online communication" might be included in the context „other legal means of communication". Communicating anonymously online is the right of each person who does not want to be identified. It is protected by constitutional provisions as long as it does not affect any other value or right protected by law, cases when the freedom of communication and the privacy of correspondence might be restricted.

In accordance with para. (2) of article 30 and para. (3) of article 32 of the Supreme Law of the Republic of Moldova, derogation from the provisions of the articles protecting these freedoms is allowed for all the actions aimed at denying and slandering the State and people, the instigation to sedition, war of aggression, national, racial or religious hatred, the incitement to discrimination, territorial separatism, public violence, or other manifestations encroaching upon the constitutional regime.

Guarantying the freedom of expression, the legislation of the Republic of Moldova is not sufficiently reflecting the online communication. In this context, state authorities might find difficulties when applying the existing domestic laws protecting the freedom of opinion and expression.
In the last years an increase of cyber crimes, international terrorism and other crimes, which might be easier committed by using the anonymously communication online has been remarked. In consequence, this problem must be analyzed at a higher level, not only national but international, too. All actions should be directed towards preventing and countering the serious, very serious and heinous crimes like international organized crimes and terrorist actions committed by using IT technologies.

Concerning the Republic of Moldova, there are several state authorities and institutions with abilities to ensure the rights of the citizens, and in necessary cases, to restrict them, protecting in this way the constitutional regime.

As regards the secure transaction and communication online, the following domestic regulations are applied:

The Government Decision no. 1176 of 22 December 2010 regarding the ability of organizations to employ encryption tools in order to secure their transactions and to communicate anonymously online, approving the Regulation on insurance secret system within public authorities and other legal entities stipulates at the Chapter VII, point 702 that "*each message containing data that can not be sent by open source must be ciphered by using the encryption tools, in order to ensure the secure transaction of information between the interested authorities*".

The Law on Security and Intelligence Service of the Republic of Moldova, no. 753 of 23 December 1999 stipulates at the article 10, letter j) that *„The Security and Intelligence Service (SIS) shall have the right to develop state codes and ciphering technical means, to execute cipher works within the Service, as well as to perform control upon the observance or compliance with the securitization regime (classification scheme) when handling the ciphered information within the cipher subdivisions of public authorities, enterprises, institutions and organizations, regardless of the type of property*".

In accordance with the point no. 5.1.3 of the National Security Strategy of the Republic of Moldova, approved by Parliament Decision No. 153 as of 15 July 2011, within its activity, SIS shall ensure the establishment, realization and development of the ciphering and technical protection systems.

According to the Government Decision no. 735 of 11 June 2002 on special telecommunication systems of the Republic of Moldova, the Security and Intelligence Service, in order to realize the national policy of special systems, defines the requirements on technical and cryptographic protection of information, undertakes necessary measures, controls and coordinates the activity of public authorities and other entities in this domain. Also, para no. 9, letter f) stipulates that the Service is responsible for determining the methods of activity with cryptographic and technical engineering security of information; coordinates the conditions of the international exchange of encrypted information.

Presenting the information above, we referred to domestic laws and regulations, related with the activity of the SIS, that permit or limit, directly or indirectly, the use of encryption technologies and services. Thus, the Security and Intelligence Service, in the frame of the competences assigned by law has abilities in protecting and keeping the confidentiality during the handling of encrypted information in the encryption subdivision of state agencies and organizations within the territory of the Republic of Moldova.

1. The Government Decision no. 965 of 11.17.2014 regarding the approving of the Regulation on organization and functioning of the automated traffic surveillance "traffic control" and the changing of the System Concept regarding automated traffic surveillance "Traffic Control", point 52 provides:

Protection of personal information in the System is performed by the following methods:
1) prevent unauthorized connections to networks and telecommunication interception by technical means of system data transmitted through them, ensured through the use of encryption methods and encryption of this information, including the use of organizational, technical and regime measures;
2) exclusion of unauthorized access to data in the system, ensured through the use of special technical means and program, encrypt this information, including organizational measures and arrangements;

2. The Government Decision no. 899 of 27.10.2014 the approving of the Regulation regarding the system on mapping of primary schools, gymnasiums and lyceums, point 54 provides:

Protection of the system information regarding education is performed in the following ways:

1) prevent unauthorized connections to networks and telecommunication interception of technical data of the system transmitted through them, ensured through the use of encryption methods and encryption of this information, including the use of organizational, technical and operating measures;

3. The Government Decision no. 716 of 08.28.2014 approving the Regulation regarding the Register of detained, arrested and sentenced persons, point 40 provides:

Protection of special categories of personal data on detained, arrested and convicted persons of SIA RPRAC is performed by the following methods:

1) prevent unauthorized connections to networks and telecommunication interception with special technical means of data from SIA RPRAC transmitted through them is ensured through the use of encryption methods and encryption of this information, including the use of organizational, technical and operating measures;

4. Law no. 91 of 27.6.2014 on electronic signature and electronic document, article 5, §(5) provides:

The electronic signature is not a means of information encryption.
(Hence it follows that encryption is not possible in the case of electronic signature.)

5. The Government Decision no. 50 of 01.15.2013 approving the Regulation regarding the procedure of issuance of visas.

Section 2. Encryption and secure transfer of data

179. In the case of representation arrangements between Moldova and other countries, cooperation between diplomatic missions and external service providers and honorary consuls, diplomatic missions shall ensure that the data is fully encrypted when they are transferred either electronically or on a physically electronic storage, from the external service provider to the diplomatic mission.

181. In third countries which prohibit encryption of data to be electronically transferred from the external service provider to the diplomatic mission, the diplomatic mission does not allow the external service provider to transfer data electronically. In this case, the diplomatic mission shall ensure that the electronic data are transferred physically in fully encrypted form on an electronic storage from the external service provider to the diplomatic mission by a diplomatic mission or consular officer, if such transfer would require disproportionate or unreasonable measures through another safe and secure way, for example by notorious carriers, experienced in transporting sensitive documents and data in the concerned third country.

182. The level of security for the transfer is adjusted in each case to the sensitive nature of the data.

183. Diplomatic missions endeavor to reach agreement with concerned third countries, with the aim of lifting the prohibition against encryption of data to be electronically transferred from the external service provider to the diplomatic mission.

184. The transmission procedure, of personal data on any storage support or by any other ways is protected in accordance with the Law on the protection of personal data and processing requirements for ensuring the security of personal data at their processing within the information systems data personal, approved by the Government.

6. The Government Decision no. 328 of 24.05.2012 on approval of the Regulation regarding the organization and operation of the automated information system "Register of forensic and criminological information".

48. Protection of the information with the criminal characteristic is performed by following methods:

1) prevent unauthorized connections to networks and telecommunication interception by technical means of data records transmitted through them, ensured through the use of encryption methods and encryption of this information, including the use of organizational, technical and operating measures;

7. The Decision of the Court of Accounts no. 47 of 02.09.2011 the audit Report regarding automated information system "Real Estate Cadastre" of the State Enterprise "Cadastre"

For data exchange between Cadastre Office and Territorial Cadastre Office, SE "Cadastre" rents VPN channels from the company "Moldtelecom", which provides a finished product. In such circumstances, SE "Cadastre" has no part in the process of encryption, transmission, decryption of data, so cannot control the quality of service and security. As a result, there is a risk that interested people from employees of the provider can intercept or modify the data. Authentication and security tools are not integrated and do not ensure an acceptable level of reliability and safety.

Recommendation 6 *Currently communications with subdivisions are organized by contracting services from the company "Moldtelecom", which provides VPN tunnels to organize data exchange. Exclusive use of the services of this company was possible because the company has not assessed the risks associated with that approach and because there is a policy of outsourcing. Direct dependence of some suppliers greatly increases the need to develop it. In addition, the company does not control the transmission and data security. To overcome the existing situation, SE "Cadastre" should implement the keys (tools) own encryption before massive data hit in the circuit data held by the supplier.*

8. The Ministry of Information Technology and Communications Order no. 106 of 20.12.2010 regarding the approval of technical regulations.

Requirements for encrypting data in databases that contain information that is not assigned to a state secret, section 6, sbp.7.

In the framework of ensuring the security of database information, the database data encryption must provide protection against unauthorized access and data integrity violations, also in the process of transmitting data through electronic communications networks.

Data encryption in the database must meet the following requirements:

- It is necessary to determine the portions of data from the database which encryption is reasonable;
- It is necessary to apply different symmetrical and asymmetrical algorithms of encryption;
- Length of the encrypted text must be equal to the length of the original text;
- Structural elements of the encryption algorithm to be invariable;
- Is necessary to ensure the necessary correction of the types and sizes of fields required from the database table in the process of encryption.
- Is necessary to ensure the integrity and strict control on the distribution of cryptographic keys;
- I case of data with high security keys from the database it is necessary to perform the change until the end of their action, after that it is necessary to perform repeated encryption of data from the database using the new key. Depending on the volume of the database data, their repeated encryption could affect their availability for an extended period of time;
- Is necessary to ensure the ability to perform selective encryption of database space spreadsheet;
- Data encryption must be performed on database server or on a separate server for encryption, and under no form at the client location.

9. Law Nr. 245 of 27.11.2008 on State Secrets

Article 35. Technical and cryptographic protection of the information defined as state secrets. The Certification of means of protecting information defined as a state secret.

(1) The technical and cryptographic protection of information defined as state secret is carried out as prescribed by the Regulation on ensuring a secret regime within the public authorities and other legal entities.

(2) Means of protecting the information defined as state secret must have the certificate of compliance with the requirements of data protection and having appropriate degree of secrecy.

(3) The organization and coordination of certification and expertise of the means of protection of information defined as state secret falls within the competence of Security and Intelligence Service. Certification is carried out in accordance with regulations and national standards in the field.

10. The Government Decision no. 856 of 21.09.2010 regarding the approval of the technical concept of the automated information system of the National Bureau of Statistics.

At the transmission of confidential information, transmitted through all channels of communication against interception, alteration or falsification of information, the information protection method will be the encryption of it and on short distance- will be the using of the protected optical fibers as communication channels. Will be used cryptographic data security means which will guarantee the necessary strength level of confidentiality and electronic key system that provides message authentication and secure exchange of information.

11. The Government Decision no. 1123 of 14.12.2010 regarding the approval of the Requirements for the security of personal data at their processing within the information systems of personal data.

Means of cryptographic protection of information containing personal data - technical means of training and technical applications, of systems and complex systems that perform cryptographic algorithms of conversion of information containing personal data, in order to ensure the integrity and confidentiality of information in processing, storage and transmission through communication channels.

Section 7

Management of user passwords

Passwords are stored in encrypted form; by using the unilateral cryptographic algorithm (hash function).

Section 12

Limit use of wireless technologies

Wireless access to information systems of personal data is documented, subject to monitoring and control.

Wireless access to information systems of personal data is allowed only in case of the use of cryptographic protection of information.

The use of wireless technologies is authorized by responsible persons of personal data holder.

64. For all the information systems categories which holds personal data

It ensures the integrity of transmitted personal data, by using the means of cryptographic protection and digital signature.

12. The Government Decision no. 834 of 07.07.2008 regarding the integrated information system of the Border Police.

Chapter VIII Ensuring information security of SIIPF

21. Informational security

Information security must be ensured through a complex system of legal, organizational and techno-economical measures with the use of different technological means, software / hardware devices and cryptographic mechanisms of information protection aimed to ensure the required level of integrity, confidentiality and accessibility of information resources.

At the development, operational and management support of SIIPF, the Border Police Department will deal with the established rules of the national legislation and standards in the field regarding the security and protection of information.