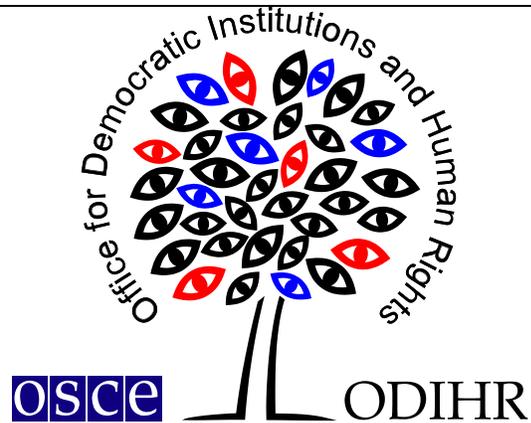Warsaw, 13 September 2005

Opinion-Nr.: FOI– MDA/038/2005 (IU)

www.legislationline.org

OPINION

ON THE DRAFT LAW OF THE REPUBLIC OF MOLDOVA

ON PERSONAL DATA PROCESSING

TABLE OF CONTENTS:

1. INTRODUCTION

1. *On 5 August 2005, the OSCE ODIHR was requested by the Ministry of Information Development of the Republic of Moldova to review the draft Law of the Republic of Moldova on Personal Data Processing (official request reference number 06/24-309).*

2. *This Opinion has been prepared on the basis on the English and Russian translations of the draft Law.*

2. SCOPE OF REVIEW

3. This Opinion analyzes the draft Law of the Republic of Moldova on Personal Data Processing (hereinafter referred to as the "draft Law") from the viewpoint of their compatibility with the relevant international human rights standards and the OSCE commitments. The Opinion also examines the draft Law in light of the international best practices with regard to human rights and data protection. The international standards referred to by the Opinion may not be only those legally binding for the Republic of Moldova, but may include international instruments not binding upon Moldova as well as documents of declarative or recommendatory nature which have been developed for the purpose of interpretation of relevant provisions of international treaties.

4. This Opinion does not purport to provide a comprehensive review.

5. The OSCE ODIHR would like to mention that the opinion provided herein is without prejudice to any further opinions or recommendations that the ODIHR may wish to make on the issue under consideration.

3. EXECUTIVE SUMMARY

6. The draft Law intends to establish a system of safeguards for the protection of the rights of an individual with regard to processing of personal data.

7. A full list of recommendations follows below.

    1) A blanket exemption for all the personal data processed "*in the framework of the national protection and security sphere*" is overly broad and it is recommended that the legislator provide for a specific and detailed list of

cases where the personal data would not fall under the law in question on the grounds on national security. [see para 12]

2) It is recommended that the draft Law include a provision for a mechanism (regular checks, monitoring, etc.) to ensure that the data undergoing processing meet the quality standards. Such a provision may possibly be added to Article 11 listing the functions and responsibilities of the oversight body in the field of data protection. Further details specific to individual types and purposes of data and individual data controllers may be provided for by the secondary legislation. [see para 15]

3) It is recommended that the Law specify the form of the consent required for the processing of personal data. The legislator may also consider the option of adding the word "informed" before "consent" to ensure that there exists sufficient understanding on the part of the data subject of the issue and the consequences of consenting, as well as to exclude cases where the person concerned is incapable of giving consent, as it may be the case with minors or otherwise legally incapable persons. The Law may make it possible for the legal guardian of an incapable person to consent on his/her behalf. In order to prevent an unnecessary increase in document flow, the Law may provide for a waiver of the requirement of separately given consent in specified cases where such consent is implied, e.g. where data processing is necessary for the performance of a contract to which the data subject is a party. [see paras 18-19]

4) It is not entirely clear from the text of the draft Law if, in cases where the consent requirement applies, the person concerned can withdraw his/her consent at any time. It is recommended that a provision entitling the data subject to withdraw his/her consent to processing of personal data at any time be added. The law may provide that the withdrawal of consent shall not have a retroactive effect. [see para 20]

5) The waiver of the requirement of consent where the data are intended for statistical or research purposes present a concern in the absence of adequate safeguards for the protection of data subjects' privacy. One such

safeguard may be a clear reference to the provision on rendering personal data anonymous ("*depersonalization*") in Article 15 of the draft Law. The Law should also make it clear that compulsory collection of personal data for statistical purposes should only be possible in cases specified by the law, and that respondents be informed of the compulsory or optional nature of the survey. [see paras 21-23]

6) While the provisions concerning the definition and treatment of sensitive data are generally consistent with the relevant international standards, the legislator might still consider further detailing these provisions with regard to data storage and transfer to third parties. It is essential that sensitive data be not stored in a file or as part of a file generally accessible to third parties. [see para 25]

7) It is recommended that the Law indicate precisely where the requests for data subject access, confirmation of data existence, rectification or erasure of data shall be addressed. The possible solutions may include the data controller ("*data holder*" in the terminology of the draft Law) itself or an intermediate body such as the regulatory body responsible for the oversight of data protection in Moldova. [see para 27]

8) It is recommended that the Law include definition of data interconnection and matching, as well as a set of specific requirements that must be met in sharing of personally identifiable data, such as a requirement of specifying the purpose and justifications for the matching program, providing descriptions of the information that will be matched, etc., and providing this information to the oversight regulatory authority, as well as making it publicly available. [see para 31]

9) It is recommended that the Law provide for public accessibility of the national registry of data controllers ("*data holders*"). [see para 34]

4. ANALYSIS AND RECOMMENDATIONS

4.1 Definition of personal data. The scope of the draft Law and its overall approach

8. The draft Law defines personal data as "*any information related to the direct or indirect identification of an identified or identifiable individual*, [including – Author's note] *the identification number of person (IDNP).*"[1] It is welcome that the definition of data is not technology-dependent, thus minimizing the risk that the definition may become obsolete with the technological advance and amendments to the law may be required.

9. The draft Law applies to both automatic and manual processing of personal data,[2] which is again welcome since even though automatic processing of information may pose greater risks in terms of privacy invasion, there is no rationale for not applying the same regulatory scheme to both automatically and manually processed files.

10. Although the draft law does not specifically make a distinction between the public and private sectors, it follows from Article 2(3)[3] that the Law intends to apply to both of these sectors which is consistent with the approach of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (hereinafter referred to as the "Data Protection Convention").[4] Exempted by the draft Law are personal data processed "*by individuals exclusively for their own use if these data are not to be disclosed*"[5] as well as personal data where these are processed "*in the framework of the national protection and security sphere, carried out at the extent set by this law.*"[6]

---

[1] Draft Law on Processing of Personal Data, Article 4.

[2] *Id.,* Article 2(1), *"The act of the present law is applied to the personal data processing, which are component parts of the evidence system or which are designated be included in such a system, processed entirely or partially by whatever medium, inclusively automatic one."*

[3] *Id.,* Article 2(3), *"The present law shall be applied to the processing of personal data, executed by any individual or legal entity."*

[4] Signed by the Republic of Moldova on 4 May 1998. See Article 3 ("*The Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sector.*") Full text of the Convention is available at http://conventions.coe.int/treaty/en/Treaties/Html/108.htm (last visited on 3 August 2005).

[5] Draft Law on Personal Data Processing, Article 2(3).

[6] *Id.,* Article 2(5). See also Article 6(2) ("*The consent of the individual is not necessary when: (a) the personal data processing is necessary for life protection, physical integrity of health protection of the interested person or other rights and freedoms; (b) the personal data processing is necessary for State security, ensuring the national security in the interests of the State monetary system or crime control; (c)*

11. Note that although the Data Protection Convention does allow to derogate from its provisions on the ground of national security, any such exemption or derogation would not contravene the Convention only as long as it complies with the requirements set out thereby, i.e. the exemption must be "*provided for by the law of the Party*"[7] as well as constitute "*a necessary measure in a democratic society in the interests of (a) protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; (b) protecting the data subject or the rights and freedoms of others.*"[8] Meanwhile, the Explanatory Report[9] to the Data Protection Convention makes it clear that "*the notion of 'State security' should be understood in the traditional sense of protecting national sovereignty against internal or external threats, including the protection of the international relations of the State.*"

12. A blanket exemption for all the personal data processed "*in the framework of the national protection and security sphere*" is overly broad and it is recommended that the legislator provide for a specific and detailed list of cases where the personal data would not fall under the law in question on the grounds on national security.

4.2 Quality of data

13. The draft Law complies with the Data Protection Convention as far as the criteria for the quality of the personal data undergoing processing are concerned. In particular, the draft Law follows that exact wording of the Convention by requiring that such data be

    1) *obtained and processed fairly and lawfully;*

    2) *collected and registered for legitimate purposes and not used in a way incompatible with those purposes;*

    3) *adequate, relevant non excessive in relation to the purpose for which they are collected and registered;*

---

the personal data, from available sources, are subject to processing, according to this law; (d) the personal data processing is done exclusively for statistic, scientific research or historic purposes.")

[7] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Article 9(2).

[8] *Id.*

[9] Full text of the document available at http://conventions.coe.int/treaty/en/Reports/Html/108.htm (last visited on 3 August 2005).

4) *accurate and, where necessary, kept up to date;*

5) *preserved in a form which permits the identification of the individuals for no longer than it is required for the purpose for which those data are collected and registered.*[10]

14. However, the draft Law as it stands now does not provide for a mechanism to ensure that the data undergoing processing meet the quality criteria. The legislator should bear in mind that the Data Protection Convention was not intended as a self-executing instrument, but rather designed to oblige the States Parties to incorporate in their domestic legislation data protection provisions to give effect to the set of principles introduced by the Convention.[11] Such provisions would necessarily require the inclusion of implementation mechanisms.

15. It is recommended that the draft Law include a provision for a mechanism (regular checks, monitoring, etc.) to ensure that the data undergoing processing meet the quality standards. Such a provision may possibly be added to Article 11 listing the functions and responsibilities of the oversight body in the field of data protection. Further details specific to individual types and purposes of data and individual data controllers may be provided for by the secondary legislation.

4.3 Data subject consent

16. The draft Law in question expressly requires the consent of the data subject before the personal data can be processed,[12] providing for an exemption from the consent requirement in the following cases exclusively:

1) *the personal data processing is necessary for life protection, physical integrity or health protection of the interested person or other rights and freedoms;*

---

[10] Draft Law on Personal Data Processing, Article 5. See also the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Article 5.

[11] See Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Article 4 ("*Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.*")

[12] Draft Law on Personal Data Processing, Article 6(1) ("*The processing of the personal data shall be executed with the consent of the interested person.*")

2) *the personal data processing is necessary for State security, ensuring the national security in the interests of the State monetary system or crime control;*

3) *the personal data, from available sources, are subject to processing, according to this law;*

4) *the personal data processing is done exclusively for statistic, scientific research or historic purposes.*[13]

17. The requirement of the consent of the data subject is a highly appropriate translation in the domestic law of the principle of authorized use of information found in the Resolution (73)22 of the Committee of Ministers of the Council of Europe On the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector,[14] and as such is to be welcomed. The draft Law also includes a highly welcome safeguard with regard to the protection of sensitive ("*special category*") data[15] by providing that *"[t]he processing, inclusively storage of special categories of personal data, shall be executed only after the written consent of the data subject."*[16]

18. However, the draft Law does not specify the form of the consent where the data undergoing processing are not categorized as sensitive, which is likely to result in difficulties with the resolution of disputes with regard to lawfulness of data processing. It is therefore recommended that the Law specify the form of the consent required for the processing of personal data. The legislator may also consider the option of adding the word "informed" before "consent," in provisions concerning both sensitive and non-sensitive data, to ensure that there exists sufficient understanding on the part of the data subject of the issue and the consequences of

---

[13] *Id.,* Article 6(2).

[14] Resolution (73)22 of the Committee of Ministers of the Council of Europe On the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector, Annex, para 5 ("Without appropriate authorisation, information should not be used for purposes other than those for which it has been stored, nor communicated to third parties."). Full text of the document is available at http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/Resolution%20%2873%29%2022.asp#TopOfPage (last visited on 3 August 2005).

[15] The draft Law on Personal Data Processing categorizes as sensitive the personal data which pertain to *"racial or ethnic origin, political opinions or religious or other beliefs, personal data concerning health or sexual life as well as data relating to criminal responsibility."*

[16] Draft Law on Personal Data Processing, Article 7(2).

consenting, as well as to exclude cases where the person concerned is incapable of giving consent, as it may be the case with minors or otherwise legally incapable persons. The Law may make it possible for the legal guardian of an incapable person to consent on his/her behalf.

19. In order to prevent an unnecessary increase in document flow, the Law may provide for a waiver of the requirement of separately given consent in specified cases where such consent is implied, e.g. where data processing is necessary for the performance of a contract to which the data subject is a party.

20. It is not entirely clear from the text of the draft Law if, in cases where the consent requirement applies, the person concerned can withdraw his/her consent at any time. While the draft Law does include a provision entitling the data subject "*to obtain rectification or erasure of personal data, if these have been processed contrary to the provisions of the present law or existing legislation,*"[17] it does not explicitly allow a data subject to request erasure of personal data in the absence of any violation of the law simply by withdrawing his/her consent. Although not explicitly required by the Data Protection Convention, such a possibility would be a logical extension of introducing the notion of consent in the Law. International best practices may provide a valuable source of inspiration for the drafter.[18] It is recommended that a provision entitling the data subject to withdraw his/her consent to processing of

---

[17] *Id.,* Article 10(1)(c).

[18] See, in particular, the Greek Law No 2472 On the Protection of Individuals with Regard to the Processing of Personal Data (Article 2(k), *"The Data Subject's Consent" shall mean any freely, given, specific and informed indication of his wishes by which the data subject, after being previously informed, signifies his agreement to personal data relating to him being processed. The rendering of such information shall include information which at least pertains to the purpose of processing, the data or the categories of data to which the processing relates, the recipients or the categories of recipients of personal data, as well as the name, trade name and the address of the Controller and his/its representative, if any. Such consent may be revoked at any time without a retroactive effect.*); Estonian Personal Data Protection Act (Art 12(4), *"A data subject may withdraw his or her consent at any time. Withdrawal of consent has no retroactive effect. The provisions concerning declarations of intention in the General Part of the Civil Code Act (RT I 2002, 35, 216; 2003, 13, 64) shall additionally apply to the consent"*); the Norwegian Act Relating to Biobanks (Article 14, *"Any person who has given their consent pursuant to sections 11-13 may withdraw such consent at any time. If consent is withdrawn, the person who gave such consent may require the biological material to be destroyed. Similarly, the donor of the material in a research biobank may require that health and personal data collected together with the material or obtained by analysis or investigation of the material are erased or returned. The right to withdraw consent or to require the destruction, erasure or return of material and data pursuant to the first or second paragraph does not apply if the material or data is anonymised, if the material forms part of another biological product after processing or if the data is already being used in scientific work. Nor does the right to require destruction apply if it has been laid down in legislation that the material or data is to be stored.")*)

personal data at any time be added. In order to prevent unreasonable increase in the workload of relevant state bodies due to frivolous requests, the law may provide that the withdrawal of consent shall not have a retroactive effect.

21. Another issue which presents a concern in the absence of adequate safeguards for the protection of data subjects' privacy is the exemption from the requirement of consent where "*the personal data processing is done exclusively for statistic, scientific research or historic purposes.*"

22. One such safeguard may be a clear reference to the provision on rendering personal data anonymous ("*depersonalization*") in Article 15 of the draft Law.[19]

23. The Law should also make it clear that compulsory collection of personal data for statistical purposes should only be possible in cases specified by the law, and that respondents be informed of the compulsory or optional nature of the survey.[20]

4.4 Sensitive data

24. As mentioned above, the draft Law on Personal Data Processing categorizes as sensitive ("*special category*") the personal data which pertain to "*racial or ethnic origin, political opinions or religious or other beliefs, personal data concerning health or sexual life as well as data relating to criminal responsibility,*"[21] and includes a welcome provision which permits processing of such data only with the data subject's consent, save for cases where

> 1) *when data processing is necessary for life protection, physical or health integrity of interested person or of another person, if the interested one is a legally incapacitated person incapable of free decision to give a written consent;*
>
> 2) *when processing refers to data, disclosed by the interested person;*

---

[19] Draft Law on Personal Data Processing, Article 15 ("*For the scientific, statistic, sociologic, medical etc. purposes, the personal data holder depersonalizes them, by withdrawing from its framework the part that permits identification of a certain individual, offering them, in such a way, an anonymous form that can not be associated with an identified or identifiable person In case of depersonalization the confidential regime, set for these data, is canceled.*")
[20] See Recommendation R(97)18 of the Committee of Ministers of the Council of Europe Concerning the Protection of Personal Data Collected and Processed for Statistical Purposes. Full text of the document is available at http://cm.coe.int/ta/rec/1997/97r18.html (last visited on 3 August 2005).
[21] Draft Law on Personal Data Processing, Article 7(1).

> 3) *when processing is necessary for preventive medicine, to diagnose, to prescribe a medical treatment for the interested person on condition that the processing of respective data shall be executed by or under the medical personnel supervision that must respect the confidential nature of the information or by any other persons that are subject to an equivalent obligation regarding confidentiality;*
>
> 4) *when law provides this necessity in order to ensure the protection of some important public interests, on condition the processing to be done lawfully, respecting the rights and guarantees of the interested individual, set by this law.[22]*

25. While the provisions concerning the definition and treatment of sensitive data are generally consistent with the relevant international standards, the legislator might still consider further detailing these provisions with regard to data storage and transfer to third parties. It is essential that sensitive data be not stored in a file or as part of a file generally accessible to third parties.

4.5 Data subject rights

26. The draft Law is fully compatible with the Data Protection Convention in delineating the rights of the data subjects. The draft sets out the following rights:

> 1) *to establish existence of personal data file, identification and habitual residence or headquarters of owner, holder or user of the file;*
>
> 2) *to obtain at reasonable intervals and without excessive delay or expense both confirmation of existence or non-existence of personal data and communication of such data;*
>
> 3) *to obtain rectification or erasure of personal data, if these have been processed contrary to the provisions of the present law or existing legislation;*

---

[22] *Id.,* Article 7(3).

> *4) to submit a request to juridical competent bodies regarding rights and freedoms violation, set by the present law.[23]*

27. However, since, as noted above, the Data Protection Convention has not been designed as a self-executing instrument, it is left up to the States to devise the specific mechanisms to put its provisions into effect. In this particular case, it is recommended that the Law (or, alternatively, the secondary legislation) indicate precisely where the requests for data subject access, confirmation of data existence, rectification or erasure of data shall be addressed. The possible solutions may include the data controller ("*data holder*" in the terminology of the draft Law) itself or an intermediate body such as the regulatory body responsible for the oversight of data protection in Moldova.

4.6 Data interconnection and matching

28. The draft Law is silent on the issue on data interconnection and matching,[24] which is a considerable gap given the seriousness of the threats posed to individual liberties by the rapidly evolving technologies by way of enabling interconnection and integration of separate record-keeping systems.

29. While it is hardly possible to contest the benefits resulting from the legitimate use of data matching – ranging from more efficient auditing to better designed social welfare programs – the law needs to provide adequate safeguards against risks posed by data matching with regard to privacy as well as due process (e.g. identification of a person as a potential violator) and the presumption of innocence.

30. The natural difficulty appreciating the incompatibilities between data across different systems – sometimes exceptionally sophisticated as it may be in the case of taxation or social welfare – and dealing with the merged data with appropriate care calls for heightened scrutiny of computer matching arrangements. Inherent risks posed by unclear, inconsistent and context-dependent meaning of data as well as low data quality multiply when placed in the context of data matching.

---

[23] Draft Law on Personal Data Processing, Article 10(1). See also Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Article 8.
[24] Data matching is understood here as the computerized comparison of separate sets of personal data, relating to the same individual but generally collected for unrelated purposes, in order to identify unwarranted differences and duplications.

31. It is recommended that the Law include definition of data interconnection and matching, as well as a set of specific requirements that must be met in sharing of personally identifiable data, such as a requirement of specifying the purpose and justifications for the matching program, providing descriptions of the information that will be matched, etc., and providing this information to the oversight regulatory authority, as well as making it publicly available.

4.7 National registry of data controllers

32. The draft Law requires that a national registry of data controllers ("*data holders*") be established and maintained by the oversight regulatory authority.[25]

33. The draft does not indicate, however, whether this registry will be accessible to the general public. Establishing a publicly accessible national registry of data controllers[26] would present an efficient practical way of giving effect to the provision of the present draft Law and the Data Protection Convention that anyone should be enabled to establish the existence of his or her own personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file.

34. It is recommended that the Law establish a publicity rule with regard to the national registry of data controllers ("*data holders*").

---

[25] Draft Law on Personal Data Processing, Article 12.

[26] The national registry is a listing of data controllers (which are usually state agencies) specifying the categories of data controlled by each listed agency as well as the purposes of their use. Making a national registry publicly available by no means implies that the data themselves should be open, but it rather clarifies which data controller is responsible for which general class of data (e.g. a Ministry of Health, national health institute or a similar state agency may be designated to handle health-related data).