National security and access to information in the Republic of Moldova

Report on compatibility of the legislation of the Republic of Moldova with the Global Principles on national security and right to information

Diana-Olivia Hatneanu
with the contribution of Mihaela Vidaicu

Chişinău 2015

This study is developed by Diana-Olivia Hatneanu with the contribution of Mihaela Vidaicu within the project "Promotion and implementation of the Global Principles on national security and right to information" with the financial support of the Soros Foundation Moldova, the Law Program.

The private institution Institute for Public Policy is a non-commercial nongovernmental, nonprofit, non-affiliated organization, aiming to contribute to development in Moldova of an open, participatory, pluralistic society based on democratic values, by developing, supporting and sponsoring research and independent analyzes of public policies in the priority areas of society.

.

IPP adress: 16/1 Puşkin str., Chişinău, Republic of Moldova
e-mail: ipp@ipp.md; www.ipp.md

CONTENTS

INTRODUCTION

The Global Principles on national security and right to information, called aksi Tshwane Principles (South Africa), published on June 12, 2013 determines a set of standards on the correlation between the need to ensure a necessary level of secure public documents that relate to national security sector, and the need to not compromise the to citizens' fundamental right to information. At the initiative of the Open Society Justice Initiative and the University of Copenhagen during September 19 to 22, 2012 European consultations on Global Principles of National Security and the right to information were held. During these meetings topics of practical application of principles have been examined and discussed. Discussions were based on a preliminary study conducted in 20 countries, including the Republic of Moldova.

Following this European initiate the problem of analysing the compatibility of national legislation with Global Principles was formulated. This report aims to analyze the issue and draw up recommendations for harmonizing Moldovan legislation with Global Principles.

The report was prepared at the initiative and with the financial support of the Soros Foundation Moldova, Law Program. During the development this Report substantial comments were formulated by Mr Viorel Cibotaru, Eugeniu Rîbca, Iurie Pîntea, Victor Munteanu, Arcadie Barbaroşie.

SUMMARY

The Global Principles on national security and right to information (TSHWANE Principles) were published on the 12th of June 2013, being developed based on the best international practice and expert opinions in this area. These principles represent standards for the development, review and implementation of national legislations in the area of access to information and national security. The aim of these principles is to regulate in details the due guarantees for the protection of the right to information in this area.

The need to establish some clear and predictable standards did appear due to the limitations imposed on the right to access to information based on motives of national security protection for the states. The aim of these standards is to provide the balance between the protection of the right to information of the people and need of the governments to classify certain categories of data from various reasons. The main goal is to provide transparency for data secrecy procedures, especially from motives of national security, in order to allow the individuals to enjoy effectively their right to information.

This report was initiated to analyze the degree of translation of the Global Principles into the national legislation of the Republic of Moldova. The aim of this report is to identify the main legislative shortcomings and to identify the most efficient solutions to adjust the national normative framework in this area. The report contains a detailed comparative analysis of the national regulations and the Global Principles.

This report analyses (1) the general principles applicable in the area of access to information, (2) categories of data which can't be disclosed based on grounds of national security and data which must be disclosed (3) rules for the secrecy and declassifying of information, (4) rules on the administration of the requests for information, (5) judiciary aspects on the national security and the right to information, (6) observatory bodies for the security sector, (7) the limits of the sanctioning or restraining measures for the disclosure of information to the public, and (8) relationships between these principles and other standards.

Thus, based on the research made, we did find the need to review the concept of national security, the current regulations being too general. This would ensure a sole and consistent approach to the limitations imposed on the right of access to information.

Also, the current provisions on the operation of the private contractors in the area of national security aren't clear enough. The principles impose also to them the responsibility to disclose data on actions which have an impact on the human rights.

In the same time, the national legislation foresees data categories which may be exempted from disclosure on grounds of national security, the task of the public authority to set the legitimacy of restrictions, as well as the obligation to motivate the denial of access to information and contains an exhaustive list of data which may be attributed to the state secret by a regulated formal procedure.

However, there's a need to regulate the public participation to the process of adaptation/review of the procedures and standards written on secrecy, as well as the obligation of public authorities to keep public lists of documents issued, which would include documents made secret.

Also, is recommended the exclusion of provisions on the extension of secrecy of information for an undefined period of time, since the extension of the maximum secrecy term shall be done only in an exceptional manner with the clear indication of the new secrecy period.

We could find that the national provisions contain regulations on the processing rules for the requests for information. However, is recommended to introduce a new emergency term to provide the answer to the request for information when the situation needs it.

The regulation of the operation for the surveillance bodies for the security sector is incomplete. Although they have been set up, their competences are limited. While at the legislative level the People's Advocate (Ombudsman) has sufficient rights to provide access to information, the subcommittee for the control of the Information and Security Service doesn't have detailed regulations, clear and accessible to the public.

The national legislation doesn't contain provisions on the categories of abuse, motives for the disclosure of information on abuse, procedures for the realization and solving of the disclosures protected internally or by surveillance bodies, protection of public disclosure, protection against sanctions for disclosure of information showing abuse, encouraging and facilitating protected disclosure, defence of the public interest for the public staff.

Although partially most of the Global Principles can be found in the national legislation, the degree of implementation of these provisions and the modality of operation of the surveillance institutions exceed the object of this report. Because of this it is recommended to ensure good implementation practice for the existing provisions and the review of the primary legislation based on the findings from this report.

At the same time, we mention that no provision for these principles shall be interpreted as restricting or limiting any right to information, recognised in conformity with the international, regional or national regulations and standards, or any norm of national or international law which would provide a greater protection for disclosures made by the public staff or other persons.

PART I. GENERAL PRINCIPLES

The obligation to provide the right to information, also in the area of national security is seen as a priority by the *Global Principles on the right to information and national security.*

Principle 1: Right to information

The first principle is formulated as follows:

" *The right to information*

a) Anyone has the right to request, receive, use and disclose information held by public authorities or on their behalf, or to which public authorities have the legal right of access;

b) The international principles recognise also that, private companies from the national security area, including private companies from the military or security area, have the responsibility to disclose data on situations, activities or actions which have an impact on the human rights;

c) Those having the obligation to disclose information in conformity with principles 1 (a) and 1 (b) must make the information available at request, while the refusal is subject to just some limited exceptions, provided by the law and necessary t prevent a specific and identifiable prejudice to some legitimate interests, including national security;

d) Only the public authorities the specific tasks of which include protection of the national security may invoke the national security as ground for the refusal to disclose information;

e) Any invoking of the national security to refuse the disclosure of some information by a private company must be explicitly authorised and confirmed by a public authority responsible for the protection of the national security.

Note: Public authorities only have the final responsibility for the national security and thus, only the Government may declare that the information can't be issued, if this could affect the national security.

f) The public authorities have also the positive obligation to publish ex officio some data of public interest."

***Information** means any original document or copy of a document material, no matter of its physical characteristics, as well as any other tangible or intangible material, no matter of the form and environment in which it is stored. This includes, but isn't limited to, records, correspondence, facts, opinions, recommendations, memorandums, data, statistics, books, drawings, plans, maps, diagrams, pictures, audio or video records, documents, e-mails, magazines, samples, models and data stored in any electronic format.*

***Information of a public interest** refers to the information which is of public interest or benefit and not solely of individual interest, the disclosure of which is "in the public interest", because, for example, because it is useful for the public understanding of the government activities.*

Public authorities *include all bodies from the executive, legislative and judiciary areas' sectors, at all levels of governance, of constitutional and legal authorities, including authorities form the area of security; and non-state structures which are held or controlled by the Government or which have the role of government agents. "Public authorities" include, also, private entities or other entities performing public functions or services or operating substantial public funds or benefits, but only in relation with the performance of these functions, provision of services or use of public funds or benefits.*

National security sector is defined as including "*i) security forces, including but not limited to army, police and other entities form the law enforcement area, paramilitary forces and intelligence and security services (civil as well as military), as well as ii) all executive bodies, departments and ministries responsible for the coordination, control and supervision of the security forces"*

Private companies from the national security sector mean "*any legal entity which makes or has made any transaction in the national security sector, but not just in that position, or as a contractor or supplier of services, facilities, staff or goods inclusively, but not limited to weapons, equipment and information. Include private military or security companies. Don't include legal entities organized as non-profit or non-governmental organizations*".

Legitimate interest of national security *refers to an interest the real aim of which and main impact is to protect national security, in conformity with the international and national laws. (Categories of Information the non-disclosure of which may be necessary to protect the legitimate interest of national security are provided by Principle 9). A national security interest isn't legitimate or its real aim or main impact is to protect an interest without any relation to the national security, such as protection of the Government or officials from embarrassing situations or from exposure to illegal activities; hiding information on the violation of human rights, any other violation of the law or of the functioning of public institutions; consolidation or perpetuation of a certain political interest, party or ideology; or the retrenchment of legal protests.*

The Resolution 1954 (2013) of the Parliamentary Assembly of the Council of Europe on national security and access to information[1] overtakes this general principle in Article 9.1 mentioning that *"any information held by public authorities must be free to access s*" and citing the Principle 1 (b) on the private players which should be assimilated to public authorities in the context of disclosure of information of public interest regarding national security.

The legislation of the Republic of Moldova provides expressly the right to access to information, in the Constitution (Art. 34), as well as in the subsequent legislation, mainly the laws specific to the area (Law no. 982/2000 on access to information[2], hereinafter the Law no.982/2000). It provides at a principle level that *"anyone* [...] *has the right to seek, receive and make known official information*"[3] (Art. 4 Para 1), in agreement with the first thesis of Principle 1 a).

[1] http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-fr.asp?fileid=20190&lang=fr

[2] Published in the Official Monitor of RM no. 88-90 from 28.07.2000.

[3] In conformity with p.6 of the Decision of the Plenary of the Supreme Court of Justice no.1 from 2007 on the review of matters on access to official information, *the notions of „oficial information" and „information of a public*

Still, Art. 5 Para 3 limits the content of this thesis, respectively of the understanding of the notion of ”anyone” only to citizens of the Republic of Moldova, as well as foreign citizens or stateless people having the domicile or residence on the territory of the Republic of Moldova. This restrain of people who can request information of a public interest may be examined in the context in which a state is responsible of the protection of the human rights, including the right to information of a public interest, only regarding persons in its jurisdiction. This jurisdiction thought, shouldn't be looked at formally, through the citizenship, domicile or residence. For example, a foreign citizen who is temporarily in another country, without having the domicile or residence in the respective state, also will have the right to life or to freedom and personal safety, being impossible to deprive him of those and considering that, through his simple location place, he is in the jurisdiction of the state.

Moreover, the limitation of the area of the requesters of information of public interest isn't provided by the *Global Principles and* neither by the Resolution PACE 1954 (2013) and appears as relevant in the context of the request of information from the area of national security, because it implies the idea of the existence of a certain link from which are flowing the duties related to the state. In the conception of the legislation of the secret information of the state, for the former communist countries, the obligation to preserve the secret character was on all citizens, not only on people with specific tasks in the area. Within such a concept might seem justified that the requesters for information which could be secret from national security motives to be in a relation of duty with the state, in order to be held in compliance with their secret character.

But the Law no. 245/2008 on the state secret[4] (hereinafter Law no.245/2008) doesn't perpetuate the above mentioned concept, because it provides as responsible for the protection of the state secret the public authorities and institutions (Art.22) and, on the other hand, obliges people having access to the state secrets in the virtue of their duties to keep this secret (Art.29). Neither the Criminal Code of the Republic of Moldova doesn't sanction but people having job tasks in the area for the unauthorised disclosure of the state secrets (Art.344 CC of RM). Or, in the conditions when the requests for access to information of a public interest are or must be followed by an analysis of the opportunity to disclose which may imply also a declassification procedure, realized by those with tasks in the area, what protects the legitimately classified information from unauthorized access s, it is unclear why only citizens of the Republic of Moldova or those with the domicile or residency here may request information. Besides, even the Law no.245/2008 allows, in emergency situations, the access s of foreign citizens to legitimately classified information, which preserves this character (Art. 28, interpreted also through Art. 2 Para2). So, even more possibility should exist for the foreign citizens to be able to request and receive information of a public interest.

---

*interest", have the meaning provided by Art.*6 *para 1) of the Law on access to information no.982-XIV from 11.05.2000. This fact results from the systematic interpretation of the Law, as well as from the EctHR caselaw (ex.: the case Sarbu vs. R. of Moldova; the case de Haes and Gijsels vs. Belgium). For consequency, is recommended to assess the information under the aspect of its „oficiality" in conformity with Art.6 of the Law, thsi being as a component part of aneentual trial relation.*

[4] Published in the Official Monitor of RM no. 45-46 from 27.02.2009.

The relevance of access to information on behalf of foreign citizens appears not only from the perspective of globalization, but, especially, taking into account the topic of information from the area of national security where a supreme interest for disclosure exists, such as those on severe violations of the human rights. That is why **it is recommended to extend the area of requesters of official information, through the removal of conditions and maintaining of the principle than anyone may request such information**. Besides, by "anyone" should be understood not only the individuals, but also legal entities, which are not covered by the requesters for information provided by Art. 5. Without any legislative modifications in this regard, the extension of the requesters for information area should be done through the application of the provisions of Article 10 of the European Convention for Human Rights, which recognises by every person, without limitation, the right to obtain information, as a part of the right to free expression.

As regards <u>those who have the obligation to disclose the information of a public interest</u>, the Law no.982/2000 provides in Art. 5 Para 2 the information suppliers:

a) "*central and local public authorities - state administration authorities, provided in the Constitution of the Republic of Moldova, i.e.: the Parliament, the President of the Republic of Moldova, the Government, the public administration, the court authorities;*

b) central and local public institutions – organizations founded by the state in the form of public authorities and financed from the state budget, which have as aim the administrative, social-cultural and other tasks of a non-commercial character;

c) individuals and legal entities which, based on the law or on the contract with the public authority or public institution, are authorized to manage public services and are gathering, selecting, possessing, storing, having at their disposal official information."

By analyzing this national legal provision against the Principle 1 b) and the definition of public authorities from the *Global Principles* we notice that the situation of the private contractors or of the non-state legal/non-state entities, which receive substantial public financing or benefits, isn't regulated but at the extent in which they are managing public services. In conformity with p. 5 of the Decision of the Plenary of the Supreme Court of Justice of the Republic of Moldova no.1/2007 on the review of matters in the access to official information[5] "*the qualification of the services provided by individuals or legal entities as being public shall be done in conformity with the second part of the legal definition, provided by Art.2 of the Law on administrative courts - «the public interest activity authorized by a public administration authority »*", what isn't covering the private contractors from the national security are. Or, **Principle 1 b) and the definition of public authorities are broader than the provision from Art. 5 Para 2 Letter c) which should be amended in the meaning of adopting the extended definition of the public authority and of the formulation from Principle 1 b) and from the Resolution 1954 (2013), with the introduction of new regulations which shall transpose also Principles 1 d) and 1 e**).

<u>The Official Information</u> is defined by Art. 6 of the Law no.982/2000 as "*all information in the possession and at the disposal of the data providers, which was developed selected, processed, systematized and/or adopted by official bodies or individuals or made available to them in the*

[5] Published in the The Bulletin of the Supreme Court of Justice of the Republic of Moldova, 2007, no.5, page 4.

conditions of the law by other legal subjects." Also, Art.6 provides that the documents carrying out information are considered:

"*1) any of the following (or a part of these):*

a) any paper or another material on which a record exists;

b) a map, a plan, a drawing, a picture;

c) any paper or another material on which are marks, figures, symbols or perforations which have a meaning for the qualified individuals to interpret;

d) any object or material from which may be reproduced sounds, images or records with or without the assistance of another item or mechanism;

e) any other data recorder, produced as result of the technological progress;

2) any copy or reproduction of the information carriers, mentioned at point 1) of the present paragraph;

3) any part of a copy or reproduction mentioned at point 2) of the present paragraph."

Article 6 regulates not only the free access to the documented information (stored in an information carrying document, but also undocumented official information, which is in the possession of the suppliers (their responsible persons). By the Decision of the Plenary of the Supreme Court of Justice of the Republic of Moldova no.1/2007, p.7, this aspect is elaborated: "*Undocumented information is the information which is not fixed on an informational support, but which the data provider has knowledge about, i.e. is its owner. The request for the provision of information can't be refused on the grounds that it is undocumented. May represent elements of undocumented information: the usage applied within the activity of the data provider; the unwritten orders of the supplier's administration on the solving of some problems related to its activity area; verbal indications of the manager of the data supplier given to an employee, etc.*" In consequence, the national Law is in conformity with the broad definition of Information provided by the *Global Principles*.

Also, Principle 1 c) is followed from the perspective of existence of the obligation to disclose information at request, the limitations being foreseen by law (the analysis of these limitations shall be done separately, within Principle 9), but also ex officio. Regarding the last aspect we have to mention that, in practice, the disclosure ex officio of some information from the area of national security, on foot of Art. 11 of the Law no.982/2000, is limited, taking into account that Para 1, pct 9), Letter d) is broad enough to cover many aspects from this area. That is why **it is recommended to realize and adopt some regulations with the power of a law, which would elaborate the obligations to disclose ex officio the information from the area of national security, starting from the information provided by Principle 10, for which there's a supreme or important interest for disclosure**.

The information and disclosure strategy from the area of defence and national security for the period 2012-2016, although providing as objective the increase of transparency degree for the national Army and institutions with responsibilities in the area of provision of national security, doesn't set specific activities for publishing ex officio for some information such as that provided by Principle 10. In consequence, is imposed the amending of the current strategy or at least to consider the introduction of such publishing activities in the future strategy.

Conclusion: *The legislation of RM corresponds partially to this principle, since shall be*

extended the area of requesters of the official information, the definition of public authorities and detailed the obligation to disclose ex officio the information from the area of national security.

Principle 2: The application of these principles

a) *These principles apply to the exercise of the right to access to information identified in Principle 1 when public authorities affirm or confirm that the information disclosure may cause a prejudice to the national security;*
b) *Taking into account the fact that national security is one of the most important public motives to restrict access to information, when public authorities mention other public motives to restrict access s – including international relations, public order, public health and public safety, law enforcement, provision of future free opinions, formulation of efficient policies and economic interests of the state – must comply with at least the standards imposed for the restriction of the right to access to information, provided by these principles, if necessary;*
c) *It is a good practice to have an accurate definition for the national security in the national legislation, in accordance with the needs of a democratic society, when it is used to limit access to information.*

National security represents one of the constitutional and legal limitations in the legal order of the Republic of Moldova, provided by Art.34 of the Constitution, by Art.7 of the Law no.982/2000 and by Art. 8 of the Law on the state security no.618/1995[6] (hereinafter "Law no.618/1995"). Still, national security isn't defined in conformity with good practice recommended by Principle 2 c), but is a broad and vaguely formulated concept. What is defined more precisely is the state security, as part of the national security, respectively as *"the protection of the sovereignty, independence and territorial integrity of the country, of its constitutional regime, of the economic, technical-scientific and defensive potential, of the legitimate rights and freedoms of the individual against informative and subversive activity of the special services and foreign organizations, against criminal attempts of groups or individuals"*[7]. Art.5 Para 3 of the Law on the Informational and Security Service of the Republic of Moldova no.753/1999[8] (hereinafter Law no.753/1999) excludes from disclosure data which might prejudice the state security.

In these conditions, when the two notions aren't overlapping, the accurate definition being in connection with the more restrained concept, is necessary a clarification and a consolidated approach to the limitation of access to information of a public interest based on motives of national security. This can be realized through the more accurate definition of national security or through the limitation of concept, when it has an impact on the free access to information, to the one of state security.

[6] Published in the Official Monitor of RM no.10-11 din 13.02.1997.
[7] Art.1 of the Law on the state security, no.618/1995.
[8] Published in the Official Monitor of RM no.156 din 31.12.1999.

Regarding compliance with Principle 2 b) is remarked the fact that Law no.982/2000 doesn't set a special regime on the request for information in the area of national security, the standards being the same regarding all information with limited accessibility.

Conclusion: *The legislation of RM partially corresponds to this principle since shall be clarified the notion of "national security" to impose a consolidated approach to the limitation of access to information of a public interest on a motive of national security.*

Principle 3: Conditions for the limitation of the right to information from the motives of national security

No restriction can be imposed on the right to information from motives of national security if the Government can't prove that: (1) the restriction (a) is provided by law and (b) is necessary in a democratic society (c) to protect a legitimate interest of national security; and (2) the Law provides adequate guarantees against abuse, including prompt, complete, accessible and effective review of the validity of the restriction by an independent supervising authority, as well as the complete review by the courts.

(a) *Provided by law*. Law must be accessible, with no ambiguity, developed with care and precision, with the aim to allow the individuals to understand what information may be not-disclosed and what information must be disclosed, as well as the actions on information which are sanctioned.

(b) *Necessary in a democratic society*.

(i) Disclosure of information must represent a real and identifiable risk for a significant damage for the legitimate interest of national security.
(ii) The risk of damage from the motive of disclosure must prevail over the general public interest of disclosure.
(iii) The restriction must comply with the proportionality principle and must be the minimum mean of restriction available against the damage.
(iv) The restriction shall not compromise the essence of the right to information.

(c) *The protection of a legitimate interest of national security*. Restrained categories of information which may be not disclosed from motives of national security must be clearly provided by law.

Note: See the definition for the term "Legitimate interest of national security" in the above section for Definitions. Principle 3(b) is more important in the case when national security isn't clearly defined in the law, as recommended by Principle 2.

The "Public interest" isn't defined in these principles. In Principle 10 is set a list of categories of public interest of special importance, which must be published proactively and should be never concealed. In Principle 37 is set a list of categories of illegal activities which represent a specific interest for the public and which the public servants must and can disclose without fear of repressions.

When balancing the risk of damages against the public interest regarding disclosure, must be taken into account the possibility to attenuate any damage following disclosure, also by means which need reasonable expenditures of funds. Hereinafter follows an illustrative list of factors which must be taken

into consideration when taking a decision on the public interest for disclosure and if it prevails over the risk of damages:

- *factors in favour of disclosure: is reasonable the assumption that disclosure may (a) promote the transparent discussion over public affairs (b) increase the responsibility of the Government (c) contribute to positive debates and inform on important problems or matters of a major interest, (d) promote the effective supervision of the public funds spending, (e) disclose motives for a Government decision, (f) contribute to the environment protection, (g) uncover threats to public health or safety or (h) uncover or help for the accountability for the violation of human rights or international humanitarian laws.*
- *factors which favour the non-disclosure: disclosure would represent, probably, a real and identifiable risk for damages brought to a Legitimate interest of national security;*
- *factors which are irrelevant: disclosure could reasonably (a) cause embarrassment or loss of trust into the Government or public servant or (b) weaken a political party or an ideology.*

The fact that disclosure could prejudice the economy of a country could be relevant to find whether the information must not be disclosed for this reason, but not for reasons of national security.

The Resolution 1954 (2013) overtakes also this general principle in Article 9.2 stating that: *exceptions from the rule of free access to information which are based on national security, or other equally important public interests must be provided by law, pursue a legitimate purpose and be necessary in a democratic society.*

Principle 3 in its first thesis is reflected in Art. 7 Para 4 of the Law no.982/2000, which provides that *won't be imposed restrictions of the freedom of information except if the data provider could prove that the restriction is regulated by an organic law and necessary on a democratic society to protect the legitimate rights and interests of the person or* ***to protect the national security*** *and that the damages brought to these rights and interests would be greater than the public interest in knowing the information*.. This covers expressly also the provision from Principle 3 b ii), underlining the importance of this special aspect of the condition of need in a democratic society.

Also, by the need to prove the fact that the prejudice brought to the rights protected by non-disclosure is greater than the public interest of knowing the information, may be understood that is covered also Principle 3 b i), because the proving can't take place without finding, in the first instance the real and identifiable risk of significant damages to the legitimate interest of national security. But, in order to be functional, the provision with the character of a general principle, respectively the application of this test in three steps ("triple test")[9], must be realised also in practice, every time the access to information is denied, based on motives of national security, as imposes the application of Principle 4 c).

Regarding the quality of the law imposed by Principle 3 a), the Law no.982/2000 as well as the special provisions from the area of secret information and of the intelligence services are in general agreement with the Principle, being accessible and quite clearly worded. Various unclear things are treated separately in this analysis, without being so serious as to affect essentially the condition of the provisions related to the limitation of the access to information.

[9] Restriction a) is provided by law; b) is necessary in a democratic society c) to protect a legitimate interest of national security.

A special Note related to accessibility refers to the secondary regulations with impact on the transparency of information for which there's an important presumption of disclosure or a major interest for disclosure, provided by Principle 10. In this regard **is recommended an careful analysis on behalf of the state authorities for all the secondary regulations** (for example: regulations, orders of managers of some authorities, internal procedures) and **the adoption of measures to make public all regulations which contain information provided by Principle 10, such as those related to the penitentiary system or procedures on the deprivation of freedom or supervision**.

Principle 3 b) iii) and iv) can be found in the legislation of the Republic of Moldova by the provision of the Law no.982/2000 in Art.7 Para 3 that *if the access to the information, documents requested is partially limited, the data providers are obliged to present to requesters parts of the document, the access to which doesn't contain restrictions in conformity with the legislation, indicating in the places of the omitted parts one of the following expressions: "state secret", "trade secret", "confidential information about an individual". The denial of access to information, for the respective parts of the document is done in compliance with the provisions of Article 19 of the present law*.

Regarding Principle 3 c), Law no. 982/2000 provides, in Art. 7, a shortlist of categories of information which may be exempted from disclosure, respectively

(1) The right of access to information may be restricted only by regulations governed by an organic law, which corresponds to the needs:
- *a) to protect the rights and reputation of another person;*
- *b) to protect the national security, public order, health or morals of the society.*

(2) In conformity with paragraph (1) of the present Article, access to official information can't be restricted, except:
- *a) information attributed to the state secret, governed by an organic law, the unauthorised disclosure or loss of which may affect the interests and/or security of the Republic of Moldova;*
- *b) confidential information from the business area, submitted to public authorities as confidential, regulated by the legislation on the trade secret, and which do not relate to production, technology, administration, finance, another activity of the business life, the disclosure (transmission, leak) of which may affect the interests of the entrepreneurs;*
- *c) information with a personal character, the disclosure of which is considered as an interference into the private life of the individual, protected by the legislation of the protection of data with a personal character;*
- *d) information related to the operative and criminal investigation of the relevant bodies, but only in cases when the disclosure of this information could prejudice the criminal investigation, intervene into the course of a court trial, deprive an individual of the right to a fair and impartial trial for his matter, or would endanger the life or physical safety of any individuals – aspects regulated by the legislation;*
- e) *information reflecting the final or intermediary results of some scientific and technical researches and the disclosure of which deprives the authors of the*

researches of the priority to publish or influence negatively other rights protected by law.

Regarding the above wording shall be mentioned the fact that national security is incident only to the exception provided by Para 2 Letter a). The other letters regulate situations where the legitimate interest protected by nondisclosure is another than the national security (the right to free competition, the right to private life, the administration of the criminal justice, the right to a fair trial, the right to life and the right to personal integrity, national economy). In these cases the refusal to disclose information shouldn't be done by invoking national security. Obviously in these situations, taking into account Principle 2 b), procedures shall be followed and guarantees shall exist provided by the *Global Principles*. A clarification of this aspect by a Decision of the Plenary of the Supreme Court of Justice of the Republic of Moldova no.1/2007 would be useful.

Consequently, in cases when national security is invoked, in conformity with the national legislation, disclosure may be refused only for that information, which is formally attributed to the state secret and, besides, the disclosure of which would bring prejudice to the protected legitimate interest, prejudice which can be prove by the application of the "triple test" provided by Principle 3. Thus, the categories of information excepted from disclosure by national security motives are limited and provided by law, also by indicating a formal procedure (classification), following Principle 3 c).

Law no.982/2000 provides, in Art.21, the remedies by which a refusal of disclosure of information based on motives of national security may be challenged:

1) *A person considering his/her right or legitimate interest affected by the data provider may challenge its actions extra judicially, as well as directly in the competent administrative court.*
2) *A person, also, may apply for the protection of his/her rights and legitimate interests to the Parliamentary Advocate (Ombudsman).*

The extrajudicial remedy refers to the challenge addressed to the manager of the data provider or his hierarchically superior body (Art.22 of the Law no.982/2000). The *Global Principles* define the **independence** of the authority provided by thesis II of Principle 3 as the quality of being free from "*influence, guidance, control of the executive, including of all authorities of the security sector*" from the institutional, financial and operational standpoint. Consequently, the extrajudicial remedy can't be defined as a guarantee against the abuse which would involve a prompt, complete, accessible and efficient verification of validity for the restriction on behalf of an independent authority.

The extrajudicial remedy meets the requirements of independence, as defined above.

The timeliness of the judicial control shall be seen first of all through the period of intimation of the court, of one month, which sets a just balance between the effective possibility of the interested party to determine the review of a limitation of the right to information based on motives of national security and the exercise prompt control. Regarding the duration of the procedure, the Decision of the Plenary of the Supreme Court of Justice of the Republic of Moldova no.1/2007 (p.2), mentions clearly that the provisions of the Law no.982/2000 are

completed by the provisions of the Law no.793/2000 on administrative courts, which sets short terms ensuring the quick review of the merits of the application (Art.22). So, the judiciary control meets also the requirement of timeliness, imposed by Principle 3 thesis II.

Regarding the extension if the judiciary control, which, through the Principle 3, thesis II, must be ”complete”, from the interpretation of the Law no.982/2000, in the light of the Decision of the Plenary of the Supreme Court of Justice of the Republic of Moldova no.1/2007, results that, on one hand, those interested may submit requests having as object any aspect they find as affecting the right to information, while, on the other hand, that the court analyses any aspect necessary for the clarification of the matter and has access s also to classified information. So, Art. 21 Para 3 provides that: *the person who considers her right or legitimate interest being affected may challenge any action or inaction of the person responsible for the receipt and review of the requests for access to information, but specifically regarding:*

a) ungrounded refusal to receive and register the request;
b) refusal to provide free unconditioned access to the public registers at the disposal of the data provider;
c) violation of the terms and procedures to solve the request for information;
d) non-presentation or the inadequate presentation of the requested information;
e) ungrounded refusal to present the requested information;
f) ungrounded attribution of the information to the category of information containing state secrets, trade secrets or to the category of other official information with limited accessibility;
g) ungrounded classification of some information;
h) setting payments and their amounts for the information provided;
i) *seeking material and/or moral damages through illegal actions of the data provider*.

Decision of the Plenary of the Supreme Court of Justice of the Republic of Moldova no.1/2007 states at p. 45 that: ”*during the review of the matter, particularly depending on the submitted requests, the court shall review and make statements over the following circumstances:*

- *the existence of the request on behalf of the plaintiff to the respondent on the provision of the official information;*
- *the term within which was provided a reply to the request, if the period in which the supplier must have sent the information did expire;*
- *whether the respondent has the information or the requested information isn't in his possession;*
- *whether the information fits into the categories of information with limited accessibility;*
- *the predominance of the public interest for disclosure of information with limited character;*
- *whether the plaintiff had or not real access to the requested information;*
- *whether the reply provided by the respondent with the information requested by the plaintiff, with the statement on the part which is not corresponding;*
- *whether the information got to the recipient in the due time;*
- *the existence and extent of the damage caused by the nun-supplying or deficient supplying of the official information;*

- *other circumstances which must be found to solve accurately the matter deduced to the court.*

Law no.982/2000 provides, in Art.21 Para (5) that *the court, during the review of the litigations on access to information, shall undertake all reasonable and sufficient cautious measures, including closed hearings, in order to avoid the disclosure of information, the limited access to which may be justified.* This provision ensures the real possibility for the court to analyse all due aspects in cases when the national security is legitimately invoked. Consequently, the court control appears as having the vocation to be "complete".

The accessibility of the judiciary control must be analyzed through the potential obstacles which the interested persons might face (such as unreasonable terms of intimation, exaggerated court costs – court fees, mandatory legal aid, etc). In the absence of these, the judiciary control answers to the accessibility requirements imposed by Principle 3, thesis II.

The analysis of the efficiency requirement for the judiciary control must be done in the light of solutions which could be provided by the court. Article 24 of the Law no.982/2000 states that *the court decides upon the application of some sanctions in conformity with the legislation, the compensation of the damages caused by the refusal to provide information or by other actions which prejudice the right of access to information, as well as the immediate satisfaction of the request of the applicant.* Shall be mentioned the fact that, this list doesn't provide expressly the declassification of information, although, on one hand, the object of the control may consist of the ungrounded attribution of the information to the category of information which contains state secrets (Art. 21 Para 3 Letter f) of the Law no.982/2000) or in the ungrounded classification of some information (Art. 21 Para 3 Letter g) of the Law no.982/2000), while on the other hand, the court is called to apply the "triple test", respectively to analyse whether, even when an information is classified, there's no public interest for disclosure which prevails. What is happening when the court finds that the requested information is state secret, that the classifying follows a legitimate interest of national security, but that there's a public interest which prevails? Will a simple court decision to disclose information be sufficient for this to happen, as long as the court didn't dispose also the declassification?

Moreover, the Law no.245/2008 states among the ground for declassification, *the existence of a decision which finds as ungrounded the classification of the information* (Art.18 Para1 Letter d). So, in order for the disclosure to happen (after declassification), the interested person should apply again to the administrative court, this time on foot of the Law no.245/2008 (Art. 17)? The Decision of the Plenary of the Supreme Court of Justice of the Republic of Moldova no.1/2007 doesn't explain this aspect. Moreover, should be noted that, in conformity with the case law of the European Court of Human Rights (...), the secret information which enters the public space loses its secret character, so that a legitimate interest to preserve the secret character doesn't justify, having to be produced the declassification.

Consequently, **to provide full efficiency to the procedure of the court review on the refusal to disclose information based on motives of national security and to avoid doubling of some procedures, Art. 24 of the Law no.982/2000 should be modified to include also the declassification of information among the solutions which the court might order.**

Regarding the control exercised by the Parliamentary Advocate (Ombudsman), provided by Art. 21 Para 2 of the Law no.982/2000, shall be noted the fact that Law no. 1349/1997 on the Parliamentary Advocates was abrogated on the 3rd of April 2014, by the coming into force of the Law no.52/2014 on the People's Advocate (Ombudsman) ("Law no.52/2014") [10]. That is why, **in order to avoid any interpretation by analogy, Art.21 Para2 of the Law no. 982/2000 must be modified to make reference to the newly-created institution**.

Even in the absence of such a legislative modification, from the general regulations for the duties of the People's Advocate results that he has the possibility to analyse also complaints on the violation of the right to information on motives of national security, respectively to refer ex officio in this regard. Regarding Principle 3, shall be mentioned the fact that the institution of the People's Advocate manifests independence characteristics imposed by it. Also, this form of control doesn't present any problems for the perspective of accessibility or timeliness of procedure, at least at the theoretical level, taking into account the novelty of the regulation. Regarding the complete character of the control performed by the People's Advocate, can be noticed the fact that, in conformity with Art.11 Letter k) of the Law no.52/2014, he has the right *to request and receive from public authorities, from persons in accountable positions at all levels, information, documents and materials necessary to exercise duties, including official information with limited accessibility and information attributed to the state secret in the conditions of the Law*. From this point of view, his control has the potential to be complete.

The limited efficiency of this form of independent control of the refusal to disclose information of a public interest based on national security motives must be examined through the perspective of the fact that the People's Advocate can issue only recommendations, although Art. 24 Para4 of the Law no.52/2014 allows him, in case he is dissatisfied of the measures taken following the recommendations, to address to a superior body and/or to inform the public opinion. The superior body isn't obliged though except to provide a reply, but not to comply with the recommendations. Also, the information of the public opinion on the information of a public interest refused for disclosure on national security motives can't function except as an extremely restrained guarantee in the meaning of compliance with the recommendations of the People's Advocate, as long as he has the obligation to preserve the secret or confidential character of the received information.

Besides the two forms of control provided by the Law no.982/2000, on the restriction of access to information based on national security motives by the Information and Security Service of the Republic of Moldova (based on Art. 5 Para 3 of the Law no.753/1999), there is also the control realised through the Sub-commission for the parliamentary control of the activity of the Information and Security Service, from the National Security, Defence and Public Order Commission, provided by the Law no.797/1996 for the adoption of the Parliament's Regulations[11]. Article 28 provides:

(1) *Within the National Security, Defence and Public Order Commission operates a Sub-commission for the Parliamentary Control of the activity of the Information and Security Service (I.S.S.).* [...]

[10] Published in the Official Monitor of RM no. 110 -114 din 09.05.2014.
[11] Re-published in the Official Monitor of RM no.50 from 07.04.2007.

(2) The Sub-commission supervises the compliance of the I.S.S. with the legality, the fundamental human rights and freedoms and democratic order in the state, ensure the political non-engagement of the I.S.S.
(3) The Sub-commission checks the compliance of the I.S.S. with the provisions of the Constitution and laws regulating the activity of I.S.S., reviews cases of violation for the Constitution, of the laws, of the constitutional rights and freedoms of the citizens.
(4) The Sub-commission members have access to secret information, signing, every separate time, an engagement to keep confidentiality of information, which represents a state secret, being accountable in conformity with legislation.
(5) The Sub-commission members may request, with the agreement of its chair, secret information and information on the current activity of the I.S.S., except information on the operative activity of the service or the identity on the persons working under cover, part of the registered staff or having specific missions which require the non-disclosure of identity.

It results that, the form of control is limited first of all by the fact that this Sub-commission can't access all information which might be relevant (see also Principle 6 and Principle 32). Moreover, it is unclear what can this Sub-commission do in the case when it finds a violation by the ISS of the right to information under national security pretexts. Although the Sub-commission doesn't have the competence to initiate an investigation in the respective situation, it can be realized through the Commission within which it operates in the conditions of Art.31 of the Law no.797/1996.

Conclusion: *The legislation RM corresponds to the conditions of the triple test, while the legal provisions from the area of secret information are clear and accessible. Also, the categories of information excepted from disclosure on the national security motives are restrictively provided by law. Although the extrajudicial remedy doesn't represent a guarantee against abuses in the current provision, the judiciary control fulfils the conditions of independence, has the vocation to be complete, and is accessible and partially efficient.*

Principle 4: The task of the public authority to find the legitimacy of any restriction

a) The burden of proof for the legitimacy of any restrictions aimed at the limitation of public access s lies on the public authority;
b) The right to information must be interpreted and applied in a broad sense and any restrictions must be interpreted narrowly;
c) In the implementation of this task isn't sufficient for a public authority to resort to the affirmation that there's a risk of prejudice; the authority has the obligation to provide specific substantive motives, to support its affirmations;

Note: Any person who requests access to information must benefit of a fair opportunity to challenge the grounds claimed for the evaluation of risks in front of an administrative and judiciary authority, in conformity with Principles 26 and 27.

d) In no case can be considered decisive the simple issue of an act by a minster or another servant, where is pretended that the disclosure of information could prejudice the national security.

The Resolution 1954 (2013) transposes this principle into Art.9.3: *limitations to the rule of free access to information, including the rule of neutrality of internet, must be interpreted narrowly. The burden of proof for the legitimacy of any restriction is on the public authority which wants to refuse disclosure.*

Article 7 Para 4 of the Law no.982/2000, sets the burden of proof for the legitimacy of limitation in conformity with Principle 4 a), as being on the public authority, no matter of the protected interest, thus, also in the case of national security. Likewise states the Plenary of the Supreme Court of Justice of the Republic of Moldova in the Decision no.1/2007, p.10: *following the provisions of Art.7 Para(4) of the Law, the data provider will have to prove in court the compliance with the elements stated in the previous point regarding the applied restriction. If the provider doesn't justify all elements or the court considers that the arguments invoked aren't convincing or are impertinent, the provider shall be obliged to release the information".* Article 7 Para 4 applies not only to the trial phase, but also in the pre-trial phase, when the data provider receives a request of official information.

Also, by a systematic interpretation of the provisions of the Law no.982/2000 can be affirmed that by rule there's a free access to information, even in the area of national security, while exceptions are of strict interpretation, in conformity with Principle 4 b).

Regarding Principle 4 c) must be stated that, besides the rule on the burden of proof presented above, Art. 19 Para 1 of the Law no.982/2000 sets the obligation to motivate the refusal: *the refusal to provide an information, an official document shall be done in writing, showing the date of the refusal, the name of the responsible person, the motive of the refusal, making a mandatory reference to the normative act (title, number, date of adoption, source of the official publication), on which refusal is based, as well as the recourse procedure for the refusal, including the limitation period*. These two provisions must be interpreted in conjunction and in the context of Principle 4 d), so that the motivation of the refusal would be detailed in substance, the simple invoking of the state secret character of information being insufficient.

Even if an evaluation of the prejudice done by the publishing of information should take place at the moment of its classification, this shouldn't generate formal refusals based on the motives of classification. The prejudice analysis must take place at each request of state secret information, while the reasoning at the basis of the refusal to disclose the information to be presented to the requester. This approach must be promoted by setting good practice and by internal regulations of the authorities managing the state secrets.

Conclusion: *The legislation of RM places the burden of proof on the public authorities to set the legitimacy for any restriction* ***and*** *the obligation to motivate the refusal, being in conformity with Principle 4.*

Principle 5: No exception for none of the public authorities

a) *No public authority – including court authorities, the legislative, the supervision institutions, information agencies, army forces, police, other security agencies, President's and Government's offices, as well as any of their component offices – can be exempted from the obligation to disclose information;*
b) *The national security doesn't represent a ground for non-disclosure of information only from the simple motive that it was generated by, or in common with, a foreign state or an inter-governmental body or a certain public authority or a unit within an authority.*
Note: Regarding the information generated by a foreign state or an inter-governmental body, see Principle 9 (a) (v).

Principle 5 is followed by the legislation of the Republic of Moldova, without exempting any authority from the obligation to disclose information.

Conclusion: *The legislation of RM corresponds fully to Principle 5.*

Principle 6: Access to information of the supervision bodies

All the institutions for supervision, petitioning [People's Advocate] *and appeal, including the courts and tribunals, must have access to all relevant information to fulfil their duties, including information of national security, regardless of the level of secrecy.*

Note: This principle is described in details in the Principle 32. It doesn't refer to the public disclosure by the supervision bodies. The supervision bodies must maintain the secret character of all the information which was classified in a legitimate manner in conformity with these Principles, as provided in Principle 35.

This aspect was analysed at Principle 3 above, in relation with the forms of control related to the access to information of a public interest and shall be analysed also in the V-th part. The courts and the People's Advocate have access to all information they deem relevant to fulfil their mandate, regardless of the level of secrecy. Instead, the Sub-commission for the control of the activity of ISS doesn't have access to all the information related to the activity of ISS, respectively to the information on the operative activities of the service or the identity of persons working under cover, being part of the registered staff or having specific missions which need the non-disclosure of identity. This is although this information is by law state secret information (Art. 16 of the Law no.618/1995 and Art. 6 Para 3 of the Law no.753/1999), while the members of the sub-commission have the right to access s state secret information, with the protection of its confidentiality. Consequently, **the limitation provided by Art.27 Para 6 thesis II of the Parliament Regulations (Law no. 797/1996) must be removed in order to comply with Principle 6**.

Conclusion: *The legislation of RM corresponds partially to the Principle 6 since not all the supervision institutions have access to relevant national security information to fulfil their duties.*

Principle 7: Resources

The States must allocate adequate resources and undertake other due measures, such as the adoption of regulations and the good administration for the archives, to make sure these Principles are followed in practice.

This principle doesn't cause serious problems at the general regulatory level, as long as in the Republic of Moldova are regulated most of the aspects provided by the *Global Principles*, including the archives administration. Where there are legislative lacks, they shall be treated at the respective Principle, and, according to Principle 7, they shall find a normative solution. Regarding the provision of resources of all types (financial, material, informational, and human); the problem is mostly in practice, and not at the regulatory level. So, **in order to comply with Principle 7, the state authorities must make sure they allocate all due resources to protect the right to information in conformity with the *Global Principles.***

Conclusion: *Weren't identified the legislative provisions contrary to this principle*.

Principle 8: State of emergency

During the state of emergency, which threatens the existence of the nation, declared officially and legally in conformity with the national legislation, as well as the international one, a state may derogate from its obligations related to the right to request, receive and disseminate information, only at the extent imposed by the exigencies of the situation and only when and for as long as the derogation is in concordance with the other obligations of the state in conformity with the international law and do not imply any discrimination.

Note: certain legal aspects related to the right to search, receive and disseminate information and ideas are so fundamental to enjoy the binding rights, that they should be always fully protected, even in situations of public emergency. As a non-exhaustive example is a part or the whole information contained in Principle 10, which has such a character.

The Law on the state of emergency, siege and war regime, no. 212/2004[12] (Law no. 212/2004) regulates the state of emergency, siege and war regime in the Republic of Moldova. In Art.5 is provided the possibility to restrain some human rights (so, also the right to information), thus:

(1) For the duration of the state of emergency, siege and war regime, depending on the severity of the situation which did determine its introduction, may be restrained, if necessary, the exercise of the rights and freedoms of citizens in conformity with Art. 54 of the Constitution.

[12] Published in the Official Monitor of RM no. 132-137 din 06.08.2004.

(2) The restrain provided at Para(1) must be in conformity with the obligations resulting from the international treaties on the fundamental human rights which the Republic of Moldova is part to and can't involve the discrimination of some persons or some groups of persons exclusively on grounds of race, nationality, language, religion, gender, political beliefs or social origin.

Principle 8 is reflected, in general, in the legislation of the Republic of Moldova. Besides, the national Law (Art. 6 din Law no. 212/2004) sets a guarantee on the compliance with Principle 8 – the information of UN Secretary General and the Secretary General of the Council of Europe on the restraining of the rights and freedoms of citizens during the state of emergency, siege or war.

Still, in order to comply with Principle 10, is necessary for at least some information of that provided by it to be with unlimited access s, neither in the situation of state of emergency, siege or war. Law no.212/2004 makes reference to Art. 54 of the Constitution of the Republic of Moldova, in conformity with which can't be restricted: the free access to justice, the presumption of innocence, the non-retroactivity of the law, the right of every citizen to know his rights and duties, as well as the right to life and physical integrity.

On the other hand, Principle 10 provides that can't be restricted in any situation, when exists a public interest for information which prevails over other interests:

- *Information on serious violations of the human rights or serious violations of the humanitarian law, including crimes in conformity with the international law and systematic and common violations of the right to freedom and personal safety.*
- *The laws and regulations which authorize the deprivation of life of a person by the state and the regulations on the deprivation of freedom, including those referring to motives, procedures, transfers, treatment or conditions of detention of the affected persons, including methods of interrogation.* Besides, Principle 10 provides, for the deprivation of freedom also that the public must have access to information on the *localization of all places operated by the state or on behalf of it where are persons deprived off their freedom, as well as identity, accusations brought motives for which are detained all persons deprived of freedom,* ***also during armed conflicts***
- *The information on the possession or procurement of nuclear weapons or other mass-destruction weapons by a state, but not necessarily about their production or operational capabilities*

To comply with Principle 10, Art. 54 of the Constitution must be interpreted in such a way that the information on the rights which can't be restrained in no situation must be disclosed, even during the state of emergency, siege or war. Still, the rights provided by Art.54 of the Constitution don't include also the right to individual freedom. So, even in the case of the proposed interpretation, isn't covered the information related to this aspect, which Principle 10 assesses as being accessible in any situation. This aspect can't be explain but by constitutional modification.

Conclusion: *The legislation of RM corresponds to Principle 8, providing also additional*

guarantees for its following. Still, for the accurate application of the Principles 8 and 10 shall be clarified the categories of information the access to which shouldn't be restrained in the situation of a state of emergency, siege or war.

PART II. INFORMATION WHICH MAY BE UNDISCLOSED BASED ON NATIONAL SECURITY MOTIVES AND INFORMATION WHICH MUST BE DISCLOSED

Principle 9: Information which legitimately may be undisclosed

a) *Public authorities may restrict the public right of access to information based on a national security motive, but only if these restrictions follow all other provisions of these Principles, information is held by a public authority and fits into one of the following categories:*

i) Information about current defence plans, operations and capacities for the duration when the information is of operational use;

Note: The expression " for the duration when the information is of operational use" has the role to request disclosure of information immediately after the information doesn't disclose anything that could be used by enemies to understand the readiness level of the state, its capacity or plans.

ii) Information about production, capacities or use of the arms systems or other military systems, including communication systems;

Note: Such information includes technological data and inventions, as well as information on production, capacities or use. The information about the budget lines related to weapons and other military systems shall be made available to the public. See in Principles 10C (3) and 10F. It is a good practice for the state to maintain and publish a control list of weapons, as encourages the treaty on the trade with weapons as conventional weapons. Also, is a good practice to publish information on weapons, gear and number of troops.

iii) Information on specific protection measures for the state territory, critical infrastructure or critical national institutions (essential institutions) against threats or use of force or sabotage, the efficiency of which depends on their secret character;

Note: The term of "critical infrastructure" refers to the strategic, active resources and systems, physical or virtual, so vital that the destruction or incapacity of such resources, goods or systems could have a debilitating impact on the national security.

iv) Information which refers to or follows from operations, sources and methods of the information services, at the extent in which they envisage matters of national security and

v) Information which envisages matters of national security which was provided by a foreign state or inter-governmental structure with an express expectation of confidentiality or other diplomatic communications, at the extent they envisage matters of national security.

Note: Is a good practice to register in writing such expectations.

Note: At the extent in which the specific information on terrorism, as well as measures to control terrorism, are covered by one of the above categories, the public right to have access to such information may be subject to some restrictions based on national security motives, in conformity with these and other provisions of the principles. In the same time,

some information on terrorism or measures to control terrorism could be of a highly increased public interest: see for example, Principles 10a, 10b, and 10h (1).

b) It is a good practice for the national Laws to provide an exhaustive list of categories of information, which is at least defined as restrained as the categories from above;
c) A state may add a category of information to the list of those from above, but only if the category is specifically identified and defined in a restrained manner and keeping the secret character of information is necessary to protect a legitimate interest of the national security which is provided by law, as provided in Principle 2 c). When a category is proposed, the state must explain how disclosure of information from that category could prejudice the national security.

Article 7 Para 2 of the Law no.982/2000 provides categories of information which are attributed to state secret and may be disclosed. Law no.245/2008 provides a list which must be interpreted as exhaustive because Art.6 provides that the legality of the classification is done through a list provided by Law. Thus, any information which can't be found in one of the set categories can't be legally classified. From this perspective is followed Principle 9 b).

This list, provided by Art.7 of the Law no.245/2008, covers the following categories:

(1) From the area of national defence regarding:
- *a) the content of strategic and operative plans, of documents related to the command with combat operations on the preparing and launch of operations, strategic deployment, operations and mobilization of troops, other important indicators characterising the organisation, number, deployment, combat and mobilization training, weapons and technical and material basis of the Armed Forces of the Republic of Moldova;*
- *b) development directions of some types of weapons, military and special equipment, their technical-tactical quantity and characteristics, organisation and technologies of production, theoretical and experimental scientific works related to the development of new models of weapons, military and special equipment or their modernization, other works planned or done in the interests of the national defence;*
- *c) civil protection forces and means, capacities at the disposal of localities and some separate objectives for the protection, evacuation and dispersal of the population, ensuring the socially vital activities of the population and the activity of production for the legal entities during war, siege or emergency, as well as in the situations of the state of emergency;*
- *d) dislocation, destination, readiness and security level for objectives with special regime, their design, construction and operation, distribution of land, subsoil and waters for such objectives;*
- *e) geodetic, gravimetric, cartographic and hydro meteorological data and characteristics which are important for the state defence;*

(2) in the area of economics, science and technology regarding:
- *a) mobilization plans and potential of the national economy, reserves and volume of supplies of strategic materials, nomenclature and generalized data about stock*

levels, amounts of deliveries, allocations, submissions, their refresh, their actual location and real amount of material reserves of the state;

b) *use of transport, communications, the potential of other sectors and objectives of the national infrastructure with the aim to ensure the capacity of state defence and security;*
c) *plans, content, volume, financing and fulfilment of state orders to ensure the state security and its defence needs;*
d) *plans, amounts and other important features on the extraction, production and implementation of strategic types of raw materials and products;*
e) *operations related to the manufacturing of the monetary signs and securities issued by the state, their storage and protection against falsification, their issue, exchange and withdrawal from circulation;*
f) *theoretical, experimental scientific works in constructions and design, based on which can be created advanced technologies, new production types, technological products and processes, which are important for the national defence and economy or which influence essentially the external economical activity, interests and/or state security;*

(3) from the area of external relations regarding:

a) *external political activity, external economical relations of the Republic of Moldova, the early disclosure of which may cause prejudice to the state interests and/or security;*
b) *military, technical-scientific or other kind of collaboration of the Republic of Moldova with foreign states and international organizations, if the disclosure of this information shall cause, inevitably, prejudice to the state interests and/or security;*
c) *external activity of the state in the financial, loans and currency areas, if the disclosure of this information shall cause prejudice to the interests and/or security of the state;*

(4) from the area of state security and provision of the legal order regarding:

a) *number, strength, content, plans, organization, financing and technical and material basis, forms, tactics, methods, means and results of information activities, of counter-information and operative investigation;*
b) *persons who did collaborate or did collaborate with the bodies implementing activities of information, of counter-information and operative investigation;*
c) *forces, means and methods to ensure state protection of victims, witnesses and other persons assisting in criminal proceedings;*
d) *protection of the state border of the Republic of Moldova;*
e) *plans, organization, financing, number of forces, means and methods to ensure the security of persons enjoying state protection and protection of their offices and residences;*
f) *government telecommunications systems and other types of electronic telecommunication networks which provide the needs of public authorities, national defence, security of the state and protection of the public order;*
g) *organization, content, condition and plans of development for the cryptographic and technical protection of the state secret, the content and results of the scientific researches in the area of cryptography, related to the state secret protection;*

h) systems and means of cryptographic protection of the state secret, design, production, production technologies for their use;
i) state ciphers, their development, creation, technologies of production and use;
j) organization of the secret regime within public authorities and other legal entities, plans and measures in the area of state secret protection;
k) other methods, forms and means of protection for the state secret;

(5) from the area of public authorities activities regarding:

a) the content of excerpts, comments, drafts, their parts, other internal documents of the public authorities, the disclosure of which could lead to the disclosure of information attributed to the state secret;
b) activity of development, modification, completion, finalization of official documents, other procedures and activities of the public authorities of data collection and processing which, in conformity with the provisions of the legislation, shall be attributed to the state secret;
c) *activity of review and deliberation within public authorities and among these in issues from areas where information is attributed to state secret.*

Besides, the Law on state security no. 618/1995 (hereinafter Law no. 618/1995) [13] (Art.16) and Law no.753/1999 (Art. 6) provide that information related to the operative activities related to the provision of the state security represents state secret, so being in general agreement with Principle 9 a).

The list provided by the Law no. 245/2008 is broader, through the proposed categories, than the one from Principle 9 a). This covers also information the disclosure of which doesn't affect only the security of the Republic of Moldova, but also the interests of the Republic of Moldova. In the same way, Art. 7 of the Law no.982/2000 allows to refuse disclosure of information attributed to state secrets if its disclosure may affect the interests **and/or** the security of the Republic of Moldova.

The notion of "interests" isn't defined, so that an unjustified extension might be reached in the area of application of the state secret and, indirectly, of the refusal to disclose information. Moreover, the concomitant/alternative use ("and/or") of notions of interests and security of the Republic of Moldova may lead to an abusive invoking of the national security to refuse disclosure of some information which doesn't affect specifically this social value. That is why, it is recommended when the refusal to disclose information is due to its secret character, to be specified clearly whether this disclosure prejudices the state security or interests.

Moreover, in conformity with Principle 9, not any information from the area of national defence is automatically excluded from disclosure, as results from the list proposed by the Law no.245/2008. Certain financial information from the area of defence, on budget lines, information about the number of troops, weapons, and equipment should be disclosed, as long as there's a supreme public interest for disclosure, also in conformity with Principle 10.

In this area is essential the specific application into practice of the "triple test", meaning also the information for which there's a presumption of a public interest for disclosure from Principle 10,

[13] Published in the Official Monitor of RM no. 10-11 from 13.02.1997.

and not the automatic application of the classification as a motive to refuse disclosure. Besides that a modification of the text of law is needed an accurate application into practice of the Law no.982/2000. This way is followed also Principle 9 c) which allows the conditioned addition of categories.

Conclusion: *The legislation of RM contains an exhaustive extended list of information which may be attributed to the state secret compared to the one covered by the Principle 9. The list covers information affecting not only the national security, but also the interests of RM. This principle is followed.*

Principle 10: Categories of information with an increased presumption or of a major interest in the favour of disclosure

Some categories of information, including those listed below, are of a specifically high public interest, taking into account their major importance in the process of democratic supervision and of the state of law. Consequently, there's a strong presumption and, in some cases, a major necessity, for such information to be public and disclosed in a proactive manner.

The following categories of information must benefit of at least one increased presumption in the favour of disclosure and may be undisclosed based on a national security motive only in exceptional circumstances and in a manner compatible with other principles, only for a strictly limited period of time, only on foot of the Law and only in the case when there are no reasonable means, by which could be reduced the prejudice which could be associated with disclosure. For certain subcategories of information, specified below as inherently subject to a supreme public interest related to disclosure, nondisclosure based on national security motives never may be justified.

A. Violations of human rights and of the international humanitarian law

1) *There's a public interest which is more important in favour of disclosure of information on severe violations of human rights or severe violations of thee international humanitarian law, including crimes in conformity with the international law and systematic and common violations of the rights to personal freedom and safety. Such information can't be refused for disclosure in no circumstances;*
2) *Information on other violations of the human rights or humanitarian law are presumed being the subject of an important presumption in favour of disclosure and, in any case, can't be refused for disclosure based on national security motives in a manner which would prevent the accountability of the guilty ones or would deprive the victim from access to an efficient remedy;*
3) *When a state is going through a justice transition process, during which the state has a specific obligation to ensure the finding of the truth, justice, repairing and guarantees of non-repeat, there's a more important public interest for disclosure, towards the society in its whole, of information on the violation of the human rights by the former regime. A succeeding government should protect immediately and preserve the integrity, issuing*

with no delay any record containing such information concealed by a former government.

Note: See Principle 21 (c) regarding he obligation to search for or reconstitute information on the violations of human rights.

4) *When the existence of violations is contested or suspected, but not found already, this principle applies to the information which, on its own or together with other information, could bring light to the truth on the alleged violations.*
5) *This principle applies to information on violations which took place or are taking place and applies no matter if the violations were done by the state holding the information or by others;*
6) *Information on violations provided by this principle include, without limitation, the following:*
   a) *A complete description and any records proving the acts or omissions which represent the violation, as well as the data and circumstances in which they took place and, if necessary, the localization of any disappeared person or of the human remains;*
   b) *Identity of all victims, as long as is protected the right to private life and other rights of victims, their relatives and of witnesses, as well as aggregated or made anonymous in another way data on the number and characteristics of victims which might be relevant in the protection of human rights;*

      Note: The name and other personal data of the victims, their relatives and witnesses may be undisclosed for the general public at the extent in which it is necessary to prevent new prejudice brought to these, if the respective people or, in case of deceased persons, members of their families, request expressly and voluntarily the nondisclosure or nondisclosure is, otherwise, obviously in correspondence with the own desires of the person or with the special needs of the vulnerable groups. Regarding victims of sexual violence, should be needed their express consent to disclose their names and other personal data. Child-victims (under 18 y.o.) shouldn't be identified for the general public. However, this principle should be interpreted, taking into account the reality that various governments in various periods did shade from the public violations of human rights by invoking the right to private life, including the people whose rights are or were rudely violated, without taking into account the real desires of the affected persons. However, these limitations shouldn't prevent the publishing of aggregated or anonymous data in a different manner.
   c) *The names of institutions and persons who did commit or were in a different way responsible for violations and, in general, of any units of the security sector, present at the moment of violations or involved in any other way, as well as of the superiors and commanders and information on the extent of the command and control;*
   d) *Information on reasons for the violations and incapacity to prevent them.*

B. Guarantees for the right to freedom and security of the person, prevention of torture and of other maltreatments and of the right to life

Information covered by this Principle includes:

1) *Laws and regulations authorising the deprivation of life of a person by the state and laws and regulations on the deprivation of freedom, including those referring to motives, procedures, transfers, treatment or conditions of detention of the affected*

persons, including interrogation methods. There's a more important public interest [than the protection of national security] *in the disclosure of these laws and regulations.*

Note: The notion of „laws and regulations", as used in Principle 10, includes all the primary or related legislation, statutes, regulations and decisions, as well as decrees and executive decisions issued by a president, a prime-minister, minister or another public authority and final and enforceable court decisions. The notion of „laws and regulations" includes, also, any rules or interpretations of the legislation considered relevant by the public authorities.

De deprivation of freedom includes any form of arrest, detention, prison or admission.

2) The location of all places where people are deprived of freedom, operated by the state or on behalf of the state, as well as the identity, and accusations brought against or detention motives for all persons deprived of freedom, including during an armed conflict.3) Information on death in custody of any person and information on any other deprivation of life which the state is responsible of, including the identity of the killed person or persons, circumstances of their death and localization of their remains.

Note: In no case may be concealed information based on national security motives which would lead to the secret detention of a person or the creation and operation of secret detention places, or secret executions. Also, there's no circumstance in which the faith or place in which any person deprived of freedom by or with the authorisation, support or express or silent consent, may be concealed by the state or refused in another way, to the family members of the person or others having a legitimate interest in the well-being of the person.

The name and other data with a personal character of the persons who were deprived of freedom, who died in arrest or whose deaths were caused by the state agents, may be concealed from the general public at the extent necessary to protect their right to private life, if the respective persons or members of their families, in case of deceased persons, request in an express and voluntary manner the nondisclosure and if nondisclosure is another modality in correspondence with the human rights. The identity of children deprived or freedom shouldn't be made available to the general public. However, these limitations shouldn't prevent the publishing of aggregated or anonymous date in another way.

C. Structure and powers of the Government

The information covered by this Principle includes, without being limited to the following:

1) *Existence of all military, police, security and information authorities and subunits;*
2) *Laws and regulations applicable to these authorities and the supervision bodies and internal mechanisms of accountability, as well as the names of officials managing such authorities;*
3) *Information necessary to evaluate and control the public funds expenditures, including the total budget, main budget lines and main information on the expenditures of these authorities;*
4) *The existence and terms of the bilateral and multilateral agreements concluded and other important international engagements of the state in matters of national security.*

D. Decisions to use military force or to procure weapons of mass-destruction

1) *Information provided by this Principle includes information relevant for the decision to engage combat troops or another military action, including the confirmation of the fact that the action was initiated, its general aim and direction, as well as an explanation of the motives for it, as well as any information which proves that a fact affirmed during the public motivation was wrong;*
   Note: The reference to the "general" dimension of the action and to the application area admits the fact that, in general, should be possible to satisfy the increased public interest to have access to relevant information for the decision to engage combat troops without disclosing all the details on operational aspects of the respective military action (see Principle 9).
2) *Possession or procurement of nuclear weapons or other weapons of mass-destruction by a state, but not necessarily details on their production or operational capacities, is a matter of public interest of the highest importance and shouldn't be kept secret.*
   Note: This sub-principle shouldn't be interpreted as support, in any way, for the procurement of such weapons.

E. Supervision

1) *The general legal framework on supervision of any kind, as well as procedures which must be followed to authorise the supervision, setting targets for supervision, as well as the use, exchange and destruction of the intercepted materials must be accessible to the public.*
   Note: This information includes: (a) laws regulating all forms of supervision, the secret ones as well as the open ones, including indirect supervision, such as the creation of profiles and extraction of data, as well as types of supervision measures which can be used; (b) admitted supervision objectives; (c) the suspicion threshold necessary to initiate or continue supervision; (d) limits on the duration of the supervision measures; (e) authorization and review procedures for the use of such measures; (f) types of data with a personal character which may be collected and/or processed in the aims of national security and (g) criteria which applies to the use, storage, erasing and transfer of these data.
2) *The public must also have access to information on the entities authorised to perform supervision and statistics on the use of supervision.*
   Note: This information contains the identity of each governmental entity which did provide specific authorisation to perform a certain supervision every year, the number of the supervision authorisations provided every year for any entity of this kind; the best information available on the number of persons and number of communications which are the object of the supervision every year; while in the case when any supervision was done without a specific authorisation – by which governmental entity.

   The public right to be informed doesn't extend necessarily over the operational fact or details of supervision done in conformity with the Law and with the obligations related to human rights. Such information may be publicly undisclosed, as well as the one on the object of the supervision at least until the moment when the supervision period ends.

3) *Moreover, the public must be informed completely on the situation of any illegal supervision. Information on such supervision must be disclosed at maximum extent without violating the right to private of those subject to supervision;*
4) *These principles envisage the public right of access to information and do not prejudice the substantial and procedural rights of the persons who were or believe they were subject to supervision;*
   Note: It is a good practice to oblige public authorities to inform persons who were subject to secret supervision (providing, at least, information on the type of measures used, dates and the body responsible for the authorization of the supervision measure) at the extent in which this can be done without endangering developing operations or sources and methods.
5) *The important presumption in favour of disclosure recognised by this principle doesn't apply to information which refers to the supervision of foreign governments' activity.*
   Note: Information obtained by secret supervision, including of the activity of foreign governments, should be subject to a disclosure in the circumstances identified in Principle 10A.

F. Financial information

The information provided by this principle includes information sufficient to allow the public to understand the finance of the security sector, as well as the rules which govern the finance of the security sector. Such information includes, without being limited to:

1) *Budgets of departments and agencies with budget lines;*
2) *Annual financial situations with budget lines;*
3) *Financial management rules and control mechanisms;*
4) *Procurement rules and*
5) *Reports of the supreme audit institutions and of other entities responsible for the control of the financial aspects of the security sector, including excerpts of any sections of such reports which are classified.*

G. Accountancy for the violations of the Constitution and of Laws, as well as other abuse of power

The information covered by this principle includes information on the existence, nature and dimension of constitutional violations or of those provided by Law, as well as other abuse of power on behalf of public authorities or staff.

H. Public health, public safety and environment protection

Information provided by this principle includes:

1) *In case of imminent or real danger to the public health, public safety or environment, all the information which may allow the public to understand or to undertake measures to prevent or reduce the damages resulted from that threat, whether the danger is due to natural causes or human activities, including the action of the state or private companies;*
2) *Other information, updated regularly, on the exploitation of natural resources, pollution and inventory of emissions, environmental impact of the large public works*

or extractions of existing or proposed resources, as well as the risk assessment and management plans for the especially dangerous facilities.

Also, the Resolution 1954 (2013) of the Parliamentary Assembly of the Council of Europe provides, in Art.9.5: *as a guarantee against too broad exceptions, access to information must be provided even in cases which normally are covered by a legitimate exception, when the public interest for the information discussed exceeds the interest of authorities to keep it secret. Such a public interest is found usually when the publication of information would:*

1) *contribute significantly to a ongoing public debate;*
2) *promote public participation to the political debate;*
3) *expose severe abuse, including violations of the human rights, other offences, abuse of a public position and deliberate concealment of some severe abuses;*
4) *improve the accountability in the management of the public matters in general and of the use of public funds specifically;*
5) *brings benefits to the public health or safety.*

In conformity with Art 9.6. of the Resolution *information on severe violations of the human rights or of the humanitarian law shouldn't be refused from disclosure based on national security motives in no circumstances.*

A part of the categories of information provided by Principle 10 can be found on the list of information which can't be attributed to state secrets, in Art.8 of the Law no.245/2008. Thus, access to this information can't be restricted by invoking its secret character, respectively the national security:

1) *Isn't attributed to state secret and can't be classified the information on:*
    a) *facts of violation of human and citizen's rights and freedoms;*
    b) *the condition of the environment, quality of food products and house appliances;*
    c) *accidents, catastrophes, dangerous natural phenomena and other extraordinary events affecting the safety of citizens;*
    d) *health condition of the population, its living standard, including nutrition, clothing, health services and social security, social-demographic indicators;*
    e) *health condition of the persons who are in positions of political appointees;*
    f) *facts of law violation by public authorities and persons in accountable positions within;*
    g) *the real state of things in the area of education, culture, trade, agriculture and public order.*
2) *Aren't attributed to state secret and can't be classified other information in conformity with the national legislation and international treaties which Republic of Moldova is party to.*
3) *It is prohibited to classify information in the case when it could limit the access to information of public interest, could affect negatively the implementation of the state and branch programs for the social-economic and cultural development or could retain the competition among companies.*

Again, the list provided by Principle 10 can't be found in full in the invoked text, which is more restrained, but, in general, the internal Law covers the same type of information for which is presumed the existence of a superior interest in favour of disclosure. And in this case, as in the case of Principle 9, is essential the application into practice of the "triple test", especially in the case of categories of information where the internal Law doesn't cover the provisions from Principle 10.

Conclusion: *The legislation of RM provides, in general, the same type of information which is not attributed to state secret and can't be classified as in Principle 10.*

PART III. A: RULES RELATED TO THE CLASSIFICATION AND DECLASSIFICATION OF INFORMATIONI

Resolution 1954 (2013) of the Parliamentary Assembly of the Council of Europe states on the rules for classification and declassification, in Art.9.4: *procedure rules for the classification and declassification of information and appointment of persons authorised to realize these tasks must be clear and accessible to the public. Information may be refused to be disclosed based on national security motives only as long as it is necessary to protect a national security interest. The public archive which contains secret information must be periodically reviewed to analyse whether the legitimacy of secrecy continues to exist based on national security motives*.

Global Principles are much more detailed regarding these obligations of the national authorities, extent in which they are followed by the legislation of the Republic of Moldova, being analysed hereinafter through the perspective of each relevant Principle.

Principle 11: Obligation to declare the motives for the classification of information

a) *Even if a state has a formal process of classification, public authorities are obliged to declare motives for the classification of information;*
   Note: "Classifying" is the process by which are reviewed records containing sensitive information and is set an index which must specify who could have access to them and the modality in which may be administered the record. It is a good practice to put in place a formal classification system with the aim to reduce the arbitrary and excessive nondisclosure.
b) *The motives must indicate the restrained category of information, corresponding t one of the categories listed at Principle 9, where the information fits in, as well as describe the prejudice, which might result from disclosure, including the degree of severity and chances for that to happen;*
c) *The secrecy level, if used, must correspond to levels* [of severity] *and chances* [to happen] *identified in the justification*;
d) *When the information is classified, i) a protecting label must be added to the record, indicating the level, if existing, and the maximum duration of classification and ii) a declaration must be included which justifies the need of secrecy at that level and for that duration.*

Note: Is encouraged the provision of a declaration which would justify each decision of classification, because this makes the public servants to provide attention to the specific prejudice which would result from disclosure and facilitates the declassification and disclosure process. Labelling paragraph-by-paragraph ensures a further coherence of the disclosure process of the needed parts of documents.

First of all, Law no.245/2008 provides a formal classification procedure, what simplifies more the discussion on the compliance with this principle, which starts from the minimum hypothesis of a lack of such a regulation. In conformity with Art. 7 Para 2 of the Law no.245/2008: *the motivation of the need to attribute the information to the state secret, based on principles of attribution of the information to the state secret and of its classification, lies on the public*

authorities and other legal entities which did develop/receive this information, being in conformity with Principle 11 a).

Moreover, also at the principle level, Law no.245/2008 (Art. 6 Para 3) enshrines argumentation as basis of the classification: *the argumentation for the attribution of information to the state secret and its classification consist in the setting of the rational character of secrecy to some specific information, eventual economic consequences and of other nature of this action, taking into account the balance between the main interests of the state, of the society and of the citizen*.

Still, Art. 6 Para 3 of the Law no. 245/2008 states about the *economic consequences and of other nature* of the classification, not about the consequences of the disclosure of information on the national security, as part of the argumentation. Adding the assessment of prejudice for the national security which could result from disclosure, including the severity level and chances for it to happen, in conformity with Principle 11 b), as part of the argumentation provided by Art.6 Para 3, would ease the application of Art.11 Para 1 of the same Law. This Article links the degree of secrecy to the severity of the prejudice caused by disclosure or loss of the classified information, as well as the application of the "triple test" in the case when is requested the disclosure of classified information.

Even though Art. 6 Para 4 of the Law no. 245/2008 provides among the Principles which are at the basis of classification also the "opportunity" defined as *setting some restrictions on the access and dissemination of the respective information from the moment of its development/receipt or in advance*, this wording is not very explicit in referring to the risks of disclosure, from the perspective of severity and chances of happening.

Art. 11 Para (1) of the Law no. 245/2008 transposes partially the Principle 11 c) providing that: *the degree of secrecy of the information attributed to the state secret must correspond to the severity of damages which may be caused to the interests and/or security of the Republic of Moldova in case of disclosure or loss of this information*. This provision doesn't make any direct reference to the motivation of the classification, as does Principle 11c) and, more important, neither for the chances for the risks produced by disclosure to happen. Since these aren't mentioned neither at the Principles of classification, it is unclear whether this analysis is taking place or not at the moment of attribution of the degree of secrecy for an information neither whether its mentioning in the classification decision is mandatory.

The first part of Principle 11 d) is followed by the legislation of the Republic of Moldova, in the sense that classified documents are marked accordingly (Art. 11 and Art. 14 of the Law no. 245/2008), but the second part on the declaration can't be found in the classification procedure.

Taking into account the above-mentioned, for a comprehensive transposition of Principle 11, would be necessary for the Law no. 245/2008 and/or subsequent internal regulations on classification to be modified to clarify the classification procedure, in the sense of existence of a mandatory written decision/declaration to classify an information, decision which would cover the elements provided by Principle 11: motives of classification, specific category of information which the classified information belongs to (a general reference to Art.7 of the Law no.245/2008 isn't sufficient), the prejudice generated by the potential disclosure, its severity and chances for it

to happen. The content of these decisions should be communicated, as much as possible, to the requesters of classified information, as motivation for the refusal to disclose what was requested.

Moreover, from the legal classification procedure results that the need to classify specific information isn't necessarily analysed and justified by the person this classification powers, who states on these aspects only at the categories level, not from case to case. This approach creates problems from the perspectives of Principle 11, in the meaning that various information, from the same category, may generate different damages, of different severities and with different chances to produce, so that the motivation of the classification, realized following the requirements of Principle 11, may be different. Or, these specific differences can't be covered by a general classification decision, at the category level, through departmental nomenclatures, for example. That is why, as much as possible, the classification decisions should be applied, at the level of information, and not at the level of category.

Conclusion: *The legislation of RM provides a formal classification procedure and enshrines the argumentation as basis for the classification. Still, Principle 11 is followed partially by the legislation of RM; although there are provisions on the corresponding labelling of the classified documents, regulations on the declaration which justifies the application of the classification are missing.*

Principle 12: Public access to the classification rules

a) *The public must have the occasion to comment the procedures and standards which regulate classification before they become applicable;*
b) *The public must have access to the written procedures and standards which regulate classification.*

Principle 12 a) must be interpreted not only in the meaning that it is necessary for the public to be consulted in a real and specific manner before adopting the regulations form the area of classification, but also before their modification. Isn't possible the classification of the adoption procedures for the rules on classification, removing this area outside the public censorship. Thus, in conformity with the Law on the transparency in the decision-making process no. 239/2008[14] (Art.7), *public authorities are obliged, if necessary, to undertake necessary measures to provide possibilities for the participation of citizens, of the associations constituted in correspondence with the Law, of other stakeholders of the decision-making process, including by:*

a. *dissemination of information regarding the annual activity programs (plans) by their placement on the official website of the public authority, by their display at its premises in an accessible public place and/or by its broadcasting in the central or local mass-media, by case;*
b. *information, as established, on the organisation of the decision-making process;*
c. *institutionalization of cooperation and partnership mechanisms with the society;*
d. *reception and review of recommendations of citizens, of the associations constituted in correspondence with the Law, of other stakeholders in order to use them for the development of the draft decisions;*

[14] Published in the Official Monitor of RM no. 215-217 from 05.12.2008.

e. *consultation of the opinion of all the stakeholders interested in the review of the draft decisions, in conformity with this law.*

To comply with Principle 12 a) is necessary the regulation of the public participation to the process of adoption/review of written procedures and standards on classification.

Regarding Principle 12 b), in general, classification procedures and standards are publicly accessible. A special attention must be provided to de detailed departmental information registers which, unlike the information register attributed to the state secret, are classified. The law provides that they must correspond to the general register, but there's no mean for the public to verify this correspondence.

Conclusion: This Principle is partially transposed into the legislation of RM since shall be clarified the public access to the detailed departmental registers and the modality of consultation in case of adoption of regulations related to classification.

Principle 13: Power to classify

a) *Only specially authorised or appointed officials, in conformity with the Law, may classify information. If an not-appointed official thinks that the information must be classified, the information may be considered classified for a short period of time and expressly defined until an appointed official will analyse the recommendation to classify;*

Note: In the absence of legal provisions which would control the power to classify, a good practice is to provide, at least, in the regulations, such a delegated authority.

b) *The identity of the person responsible for the decision to classify must be indicated or identifiable on the document, to ensure the accountability, if there are compelling reasons to hide the identity;*

c) *The officials appointed by Law must attribute the original power to classify to a small number of high-rank subordinates, efficient from the administrative perspective.*

Note: It is a good practice to publish information about the number of persons who have the authority to classify, as well as the number of persons who have access to classified information.

Law no. 245/2008 isn't very specific in appointing persons with the authority to classify information. The classification process is produced through information registers, the register of the information attributed to the state secret including also public authorities with powers of disposal on this information. These are very general though, indicating institutions, nu persons (by functions and positions, non-nominally), while the right to use classified information doesn't necessarily provide the authority to classify.

The subsequent registers, which are approved by persons in accountable positions in the area (unidentifiable) are classified, so that, even if they contain more indicators to the persons

authorised to classify information, they can't be evaluated through the perspective of Principle 13. In the end, those who are applying the secrecy labels on the material information carriers, by transposing registers, are those who are developing/receiving information, so, theoretically, all persons of an institution who have powers related to the development/receipt of information. Correlated with the provision from Art.13 Para 4 of the Law no. 245/2008, there can't be but those persons who may have access to state secrets, respectively those with positions provided in the special registers, drawn by the managers of the bodies they are working in.

The sole specifically indicated persons are those from the register of persons in accountable positions invested with the powers to attribute information to the state secret. These are:[15]

1) The President of the Republic of Moldova
2) The Chair of the Parliament
3) The Prime-minister
4) Members of the Government
5) The Secretary General of the Government
6) The Chair of the Constitutional Court
7) The Chair of the Supreme Court of Justice
8) The Chair of the Court of Accounts
9) The Prosecutor General
10) The Governor of the National Bank of Moldova
11) The Director of the Information and Security Service
12) The Director of the State Protection and Guard Service
13) The Director of the Special State Couriers Service
14) The Director General of the State Administration of Civil Aviation
15) The Director General of J-s.C. "Moldtelecom"
16) The Chair of the National Commission for the Financial Market
17) Managers of other central authorities administrative institutions provided in Art.24 of the Law no.64-XII from 31st of May 1990 on the Government
18) Heads of central and local public authorities, other legal entities of public and private law appointed to handle information attributed to state secret, in conformity with the provisions of the register of information attributed to state secret, approved by Government Decision no.411 from the 25th of May 2010

From the provisions of the Law no.245/2008, results that these persons may delegate classification powers to other persons.

As long as the classification is realized through registers and only persons mentioned above or their delegates may approve such registers, Principle 13 a) thesis I is followed. Regarding thesis II, the Law no. 245/2008 is much more specific, respectively it provides, at Art. 12, that, in case when the person developing/receiving information can't identify an applicable category in the registers, the person in the accountable position from the public authority has the obligation to provide the preliminary classification, while in one month term having the obligation to address to the person in accountable position who did approve the register, a proposal on its modification/completion. In the next 3 months, the person who did approve the register either

[15] Government Decision no.449/2011 on the Register of persosn in accountable positions with powers to attribute information to the state secret, Published in the Official Monitor no.103-106 from 24.06.2011.

decides to modify/complete it or to remove the secrecy stamp from the material carrier of the information, what is equivalent with the removal of the secret character. This way is followed Principle 13 a) thesis II.

Principle 13 b) is also followed, Law no. 245/2008 providing, in Art.14 Para 1 that the material carriers of the classified information must contain *the position, name, surname and signature of the person in accountable position who did classify the information*. Moreover, Para 3 provides that if the provision can't be realized directly on the material carrier, it will be indicated in the accompanying documentation.

Regarding compliance with Principle 13 c), this is hard to evaluate based on the public information on procedures and standards of classification and it also can't be found at the principle level in Law no. 245/2008, a lack which should be removed at the regulatory level. Moreover, a good practice for the application of this principle imposes the publishing of the number of persons who have the authority to classify information, as well as the number of persons who have access to the classified information, a good practice which is not applied in the Republic of Moldova.

Conclusion: *Principle 13 a) and b) is transposed into the legislation of RM. The compliance with Principle 13 c) is hard to evaluate based on the existing public information.*

Principle 14: Facilitation of internal appeals against classification

The public staff, including that affiliated to the security sector, who thinks that information was classified inadequately, may challenge the classification of information.
Note: The staff employed in the security sector is the first one who must be encouraged to challenge classification, taking into account the big increase of classification in the security agencies, the fact that most of the countries didn't set or appoint an independent structure to receive complaints on behalf of the staff employed in the security sector, as well as disclosure of secret information many times leads to bigger sanctions than the disclosure of other information.

Law no. 245/2008 provides an appeal procedure against the decision to classify information (Art. 17), but it is general, being accessible to any citizen or any legal entity. There are no specific provisions for public staff, including those affiliated to the security sector, and it is hard to believe that they will use the legal procedure which provides, in some situations, to appeal to their own boss and then to court, especially if the improper classification was done with a bad will, and not by mistake.

The difficulty comes, on one hand, from the internal culture of keeping the secret where these people work, as well as from the sanctions they could be exposed to. That is why, would be appropriate the introduction of a procedure, similar to the one of whistleblower, for the internal appeals against improper classification.

Conclusion: *This principle is partially followed, since there are regulations on a general appeals procedure against decisions to classify information, but aren't known any special provisions for public staff, including the one affiliated to the security sector.*

Principle 15: Obligation to store, manage and preserve information on national security

a) *Public authorities have the obligation to store, manage and preserve information on in conformity with international standards. The information may be excluded from storage, administration and preservation only in conformity with the Law;*
b) *Information must be administered accordingly. The filing systems must be consequent, transparent (without disclosing legitimately classified information) and complete, so that specific access requests would lead to the identification of all relevant information even if information isn't disclosed;*
c) *Each public entity must create and make public, as well as review and update periodically, a detailed and accurate list of classified documents which are handled by it, less of those documents with an exceptional character, the simple existence of which can't be legitimately disclosed in conformity with Principle 19, if it exists.*

Note: It is a good practice to update these lists.

The storage and administration of the classified information is realized in conformity with the conditions of the Regulations on the provision of the secrecy regime within public authorities and other legal entities[16], quite detailed conditions, so that Principle 15 a) and b) is followed.

Regarding the publishing of a detailed list of all classified documents held by each public entity, the list must be periodically reviewed, this obligation isn't provided by the legislation of the Republic of Moldova. Moreover, neither detailed registers, based on which these documents were classified aren't public. The obligation from the Law no.982/2000 Art.11 Para 5, to develop guidelines with lists of disposals, decisions and other official documents issued by an institution is too general and doesn't refer expressly to the classified documents. Or, in this area, meaning also the sanctions to which is exposed the person who discloses without authorisation a secret information, is necessary a specific regulation. Consequently, Principle 15 c) isn't followed, so that is necessary to modify Law no.245/2008 to include such an obligation and Law no.982/2000 to include also documents classified among them contained in the public lists of issued documents.

Conclusion: *The legislation of RM corresponds partially to Principle 15. Although providing detailed conditions for the storage and administration of the classified information, it doesn't provide the obligation of public authorities to keep public lists of issued documents.*

Principle 16: Time limits for the secrecy period

[16] Approved by Government Decision no.1176 from 22.12.2010, Published in the Official Monitor of RM no. 139-145 from 26.08.2011.

a) *Information may be refused from disclosure based on national security motives only as long as it is necessary to protect the legitimate interest of national security. The decisions to refuse must be reviewed periodically to provide the compliance with this Principle;*

Note: It is a good practice for the review to be requested through the statute at least once every five years. Many countries request the review in shorter periods of time.

b) *The one who is classifying must provide the date, the conditions or event when the classification ends;*

Note: It is a good practice for this time limit or provision of some conditions, or the expiry event to be subject to periodical reviews.

c) *No information can stay classified indefinitely. The maximum presumptive classification period based on national security motives must be set by Law;*

d) *Information may be restricted beyond the presumptive deadline only in exceptional circumstances, in conformity with a new decision to restrict access, taken by another decision-maker, who would set a new period.*

From the common interpretation of Art.7 Para 2 of the Law no.982/2000 and of Art.18 of the Law no.245/2008, results that, in principle, a classified information may be disclosed in the moment when is no longer necessary the classification to protect the legitimate interest of national security. This is possible only if a formal process of declassification takes place. In principle, nothing prevents an authority which did receive a request for information which is formally classified, to review at that moment the need to maintain secrecy. Even if this isn't expressly provided by Law no. 245/2008, it results from the fact that Law no. 982/2000 provides the application of the "triple test" before limiting the access to an official information. At what extent happens this review in practice is hard to assess and is needed the promotion of the good practice in this regard, to comply with Principle 16 a) thesis I.

Regarding the periodical review of the refusals to disclose classified information, this isn't provided by the national legislation, Principle 16 a) thesis II being unfollowed. The obligation of periodical review refers to the registers with information, thus, to categories of information which are subject to classification. This obligation doesn't refer to refusals to disclose information nor to the classified information itself. That is why, **the Law must be modified in the sense of introducing this obligation to review the classified information itself, or the refusals to disclose classified information.**

The time limit for the classification is mentioned on the material carrier of the classified information, in conformity with Principle 16 b) (Art.14 Para 1 of the Law no. 245/2008).

The information may remain classified for an indefinite period, contrary to Principle 16 c) thesis I, even if there's a maximum presumptive period of secrecy, provided by Law. This is because Art.13 of the Law no. 245/2008, after providing these maximum classification periods, introduces the possibility to extend them, without having any conditioning for this extension, for example the period for which it can be done, contrary to Principle 16 d). Moreover, the information about persons who are collaborating confidentially with the bodies carrying out activities in the intelligence (information) area, counter-information and operative investigations are classified indefinitely.

In these conditions **is necessary the modification of Art.13 of the Law no. 245/2008 to put it into conformity with Principle 16 c) and d). The extension of the maximum classification period may be dome only in exceptional circumstances, by another decision maker and with the clear indication of the new classification period.**

Conclusion: *This principle is partially transposed into the national legislation. Although is provided a formal procedure of declassification, the national legislation doesn't provide the obligation of periodical review for the refusals to disclose classified information. Moreover, information may stay classified for an undefined period, contrary to Principle 16.*

Principle 17: Declassification procedures

a) The national legislation must provide the Government responsibility to coordinate, supervise and implement governmental declassification activities, including regular improve and update of the instructions for declassification.
b) Must be set up procedures for the identification of the classified information of a public interest for priority declassification. If the information of a public interest, including information which fits one of the categories listed in Principle 10, is classified dues to some exceptional sensitivities, it must be declassified as soon as possible;
c) The national legislation must set up procedures for block declassification;
d) The national legislation must set up fixed periods for an automatic declassification for various categories of classified information. In order to decrease the burden of declassification, information must be declassified automatically, whenever possible;
e) The national legislation must set up an accessible and public procedure for the requests for declassification of documents;
f) Declassified documents, including those declassified by courts, tribunals or other supervision bodies, parliamentary advocates or courts of appeal should be disclosed in a proactive manner or made available to the public in another modality (for example, by harmonising the legislation in the area of national archives or access to information, or both).

Note: This principle doesn't affect the provisions on the other motives for nondisclosure provided in the preamble of paragraph 15.

Note: Good additional practices include the following:
- *periodical review of the use of new technologies in the declassification processes; and*
- *regular consultations with people with professional experience regarding the process of setting priorities for declassification, including automatic declassification, as well as block one.*

Law no. 245/2008, in Art.5, provides the powers of public authorities in the area of protection of the state secret, but direct reference to the declassification is limited. Only in the case of the President of the Republic of Moldova the Law mentions explicitly the powers related to solving problems arising in relation to declassification and protection of information (Art.5 Para2 Letter c). Also, the same Article provides, in Para 6, in the task of Inter-departmental Commission for the Protection of the State Secret, the control on *terms of validity for the secrecy stamp set previously for the protected information*, what provides practically a control of classification.

Article 18 of the Law no.245/2008, provides in more accurate terms, in Para2-3, the authorities with powers of declassification:
(*2) Declassification of information is done by people in accountable positions with powers to classify the respective information.*
(3) The Interdepartmental Commission for the Protection of the State Secret, as well as the heads of public authorities and of other legal entities are empowered to declassify information which was classified without grounds by subordinated persons in accountable positions.
(4) The managers of the state archives have the power to declassify the material carriers of information attributed to the state secret which are stored in the closed funds of the archives, with the condition that the founding organisation of the fund or its legal successor delegate them such powers. In case of liquidation of the organisation-founder of the fund or absence of its legal successor, the declassification matter for the material carriers of information attributed to state secret is reviewed by the Interdepartmental Commission for the Protection of the State Secret.

Also, Art.10 Para 5 of the Law no. 245/2008 provides that: *heads of public authorities with powers of disposals over the information attributed to state secret are obliged to review periodically, at least once every 5 years, the content of departmental registers of information which shall be classified for the argumentation of classification of information and correspondence to the secrecy grades set previously.*

Thus, from the corroboration of the above provisions results that, in general, Principle 17 a) is followed. Instead, Principle 17 b) can't be found in the legislation of the Republic of Moldova. Law no.245/2008 shall be modified, in the sense of including an obligation for the authorities with classification powers to actively identify and analyze the opportunity of declassification with a priority for the information of a public interest from the area of national security, especially of those from the categories provided by Principle 10.

Principle 17 c) is followed, as long as the review of the registers of various importance levels and the eventual elimination of one or more categories of documents, as well as the modification of Art.7 and 8 of the Law no.245/2008 represents specifically such group declassifications, and not document by document ones.

Article 18 Para 1 Letter a) of the Law no. 245/2008 provides as ground for declassification the expiry of the classification period, what should presume an automatic declassification. But nowhere is specified whether, upon the expiry of the respective terms, declassification produces automatically or whether a special procedure is needed. Isn't specified any obligation of active disclosure of information declassified after this moment. Consequently, for a complete

transposition of Principle 17 d) and f), such a clear provision must be included into the Law no. 245/2008.

Regarding the declassification requests, the procedure is clearly provided by Law, in conformity with the requirements of Principle 17 e):

(1) Any citizen or legal entity has the right to apply to persons in accountable positions who did classify certain information with a motivated request for the declassification of this information. The respective persons in accountable positions are obliged, in one month period, to provide a written reply to the citizen or legal entity on this request.

(2) Persons in accountable positions who are shirking from the substantive review of the request are liable in conformity with the legislation.

(3) The decision to classify information may be challenged at the hierarchically superior body or person in an accountable position, at the Interdepartmental Commission for the Protection of the State Secret or administrative court. In case of rejection of the request submitted in a hierarchic order, the citizen or the legal entity has the right to challenge in the administrative court the decision of the hierarchically superior body or person in accountable position. If one of these authorities finds the classification as ungrounded, the respective information shall be declassified in conformity with the present Law.

(4) *The administrative court reviews the request in conformity with the provisions of the Law on administrative courts no.793-XIV from the 10th of February 2000."* (Art.17 of the Law no. 245/2008).

Conclusion: *The legislation of RM corresponds partially to Principle 17. Although the national legislation provides the authorities with declassification powers, it doesn't provide their obligation to analyse the opportunity of declassification, with priority, for the information of public interest from the area of national security. Moreover, the national legislation doesn't specify whether after the expiry of the classification period the declassification produces automatically.*

PART III. B: RULES FOR THE ADMINISTRATION OF THE REUESTS FOR INFORMATION

As a general principle, Resolution 1954 (2013) of the Parliamentary Assembly of the Council of Europe provides in Art.9.8: *requests for access to information must be analysed in a reasonable period of time. Decisions to refuse access must be well grounded, subject to appeal in front of an independent national authority and in the end subject to court review. When receiving a request for information, the public authority must in principle confirm or deny the holding of the requested information.*

The Global Principles are much more detailed regarding these obligations of the national authorities, the extent in which they are followed by the legislation of the Republic of Moldova being analyzed hereinafter through the perspective of each relevant Principle.

Principle 18: The obligation to take into consideration the request, even if the information was classified

The fact that the information was classified isn't decisive in determining the modality to answer to a request for information. The public authority holding the information must take into consideration the request in conformity with these Principles.

Law no. 982/2000 provides the obligation to analyse any request for information in Art.15 Para 2. For requests referring to classified information, this necessity results with enough firmness also from the wording of paragraphs 3 and 4 of Art.7: (3) *If the access to requested information, documents is partially limited, the data providers are obliged to present to the requesters parts of the document, access to which doesn't contain restrictions in conformity with the legislation, indicating in the places of the omitted parts one of the following phrases: "state secret", "trade secret", "confidential information about an individual". Refusal for access to information, for the respective parts of the document is drawn following the provisions of Article 19 of the present Law.*
(4) There will be no restrictions imposed on the freedom of information unless the supplier may prove that the restriction is regulated by an organic Law and necessary in a democratic society to protect the legitimate rights and freedoms of the individual or national security protection and that the prejudice brought to those rights and interests would be greater than the public interest of knowing the information.

Obviously neither the partial access nor the application of the "triple test" can't be realized in the absence of an effective analysis of the request for information. Consequently, at the legislative level, Principle 18 is followed. It is necessary though, for this Principle to be promoted also in practice, by the corresponding training of the servants charged with analysing requests for official information. Moreover, these servants must have access themselves to the information in order to be able to realize the analysis or for those having access to classified information to know and apply also the legislation on access to information.

Conclusion: *At the legislative level this principle is followed.*

Principle 19: Obligation to confirm or deny

a) *When receiving a request for information, the public authority must confirm or deny the possession of the requested information.*
b) *If in a legal system exists the possibility that, in extraordinary circumstances, to be classified the existence or non-existence of a certain information in conformity with Principle 3, then the refusal to confirm or deny the existence of information as a reply to a certain request must be based on the presentation of the motives for which the simple confirmation or denial of existence of information would endanger a distinct category of information, which is set as needing such an exceptional treatment in the national legislation.*

In conformity with Art.19 Para 1 of the Law no. 982/2000, any refusal to disclose an information, so also the one referring to the classified information, must be disclosed in writing and motivated. The Decision of the Plenary of the Supreme Court of Justice of the Republic of Moldova no.1/2007, p. 33, clarifies also the situation by Principle 19 b): *refusal to present information could be exercised, without indicating the fact whether the supplier holds or not the information with limited accessibility, only in certain circumstances, when can reasonably be supposed that recognising the existence or inexistence of this information, itself, may represent a dangerous disclosure for legitimately protected interests*.

Consequently, Principle 19 is followed partially. For a complete transposition would be necessary for the Decision of the Plenary of the Supreme Court of Justice of the Republic of Moldova no.1/2007 to be supplemented in the sense of introducing the obligation for motives for which the simple confirmation or denial of existence of information would endanger a distinct category of information.

Conclusion: *Principle 19 is transposed partially in the national legislation. Although there are provisions on the form of refusal to disclose information, isn't provided the obligation to invoke motives for which the simple confirmation or denial of existence of information would endanger a distinct category of information.*

Principle 20: Obligation to present in writing the motives for the refusal

a) *If a public authority refuses the disclosure of certain requested information, in full or in part, it should specify in writing the motives for this, in conformity with Principles 3 and 9, within the period of time provided by the Law on the disclosure of information;*

Note: See Principle 25 in which the requirement for the time in which the reply must be submitted must be provided by Law.

b) The authority must also provide the requester with enough information on the servant/servants who did authorise the refusal and the process by which refusal was reached, only if it through itself wouldn't disclose classified information, as well as ways for appeal, to allow the analysis of compliance with the Law of the authority.

In conformity with Art.19 Para 1 of the Law no. 982/2000 "*refusal to provide an information, an official document shall be done in writing, indicating the date of the refusal, name of the responsible person, motive of refusal, making a mandatory reference to the normative act (title, number, date of adoption, source of the official publication), which the refusal is based on, as well as the recourse procedure for the refusal, including the limitation period*." Consequently Principle 20 is fully followed.

Conclusion: *At the legislative level this principle is followed.*

Principle 21: Obligation to recover or restore the missing information

a) When a public authority can't localize the information which would answer a request while the records containing the information should have been preserved, collected or produced, the authority must undertake reasonable efforts to recover or restore the information for a potential disclosure by the requester;

Note: This principle applies to information which can't be localised because of a certain motive, for example, because it was never collected, was destroyed or are undetectable.

b) A representative of the public authority may be requested under oath, in a reasonable period of time, and provided by law, to present all procedures implemented to try and recover or restore the information in a manner, which would allow for those procedures to be subject to court review;

Note: When can't be found information which must be maintained by Law, the problem should be addressed to the police or administrative authorities for investigation. The result of the investigation must be made public.

c) The obligation to recover information is specifically important i) when the information refers to the suspected severe and systematic violations of the human rights and/or ii) during the transition to a democratic form of governance, from a governance characterised by large violations of the human rights.

Principle 21 cannot be found in the legislation of the Republic of Moldova, Law no. 982/2000 should be modified to include also this obligation of recovery or restoring of information, in the case when the information can't be localized, although it should have been preserved, collected or produced.

Conclusion: *The legislation of RM doesn't provide the obligation to recover or restore information.*

Principle 22: Obligation to disclose parts of documents

Exceptions from disclosure apply only to specific information specific and not full documents or other records. May be undisclosed only specific information the restriction validity of which was proven ("information exceptions"). In the case when a record contains information exceptions, as well as information which doesn't represent exceptions, the public authorities have the obligation to extract and disclose the information which doesn't represent exceptions.

Article 7 Para 3 of the Law no. 982/2000 provides that: *if the access to requested information, documents is partially limited, data providers are obliged to present to the requesters parts of the document, access to which doesn't contain restrictions in conformity with the legislation, indicating instead of the omitted parts one of the following phrases: "state secret", "trade secret", "confidential information about an individual". The refusal of access to information, for the respective parts of the document is drawn in compliance with the provisions Article 19 of the present Law.*

Also, Law no. 245/2008 provides, in Art.11 Para 3 and 4 that: *(3) Isn't allowed the application of secrecy stamps mentioned at Para(2) in order to classify the information which isn't attributed to the state secret.*
(4) Pages, paragraphs, sections form a certain document or from annexes to it may need the attribution of different secrecy levels and must, in this case, carry the corresponding mention. The level of secrecy attributed to the document as a whole coincides with the one of its part which was attributed the highest secrecy level."

From the corroboration of the two texts results that access to classified parts of documents not only is provided by law, but also is technically possible, as long as a document containing classified parts as well as unclassified ones will carry the corresponding labels on each part. Consequently, Principle 22 is followed.

Conclusion: *At the legislative level this principle is followed.*

Principle 23: The obligation to identify the undisclosed information

A public authority holding information which it refuses to disclose must identify that information as specifically as possible. At least the authority must disclose the quantity of information it refuses to disclose, for example through the estimation of the number of pages.

Principle 23 can't be found directly in Law no. 982/2000, only indirectly, through the obligation to motivate the refusal. Article 19 of this Law and/or Decision of the Plenary of the Supreme Court of Justice of the Republic of Moldova no.1/2007 thus must be modified and completed in such a way, so that they would contain the specifications from Principle 23.

Conclusion: *The legislation of RM doesn't provide the obligation to identify information as specifically as possible.*

Principle 24: Obligation to provide information in an available format

Public authorities must disclose information in the format preferred by the requester at the extent of possibility.
Note: This includes, for example, the obligation of the public authorities to undertake corresponding measures to provide information to persons with disabilities, in an accessible format and technologies timely and with no additional costs, in conformity with the UN Convention on the Rights of Persons with Disabilities.

Article 12 Para 2 of the Law no. 982/2000 provides in the duty of the requester to include in the request for information the acceptable modality to receive requested information. Article 13 Para 2 also provides in the task of public authorities the correlative obligation: *excerpts from registers, documents, information (some parts of those), in conformity with the request of the applicant, may be made available to the respective person, in a reasonable form, acceptable by the latter, in order to be:*

a) *reviewed on the premises of the institution;*
b) *typed, photocopied or copied in another way, which would ensure the integrity of the original;*
c) *recorded on an electronically carrier, recorded on video, audio tapes, another carrier produced by the technological progress.*

Conclusion: *At the legislative level this principle is followed.*

Principle 25: Deadlines to answer to requests for information

a) *The deadlines to answer requests, also in substance, for the internal control, for the decisions of the independent body, if it exists, and for the judiciary control must be set by Law and must be as short as it is practically possible;*

Note: In conformity with the requirements set in most laws on access to information, the best practice is considered to provide twenty working days or less as a time period in which a reply on substance must be provided. In the case when the deadlines to answer requests aren't provided in the Law, the deadline should be of not more than 30 days for a standard request. The laws may provide different deadlines, taking into consideration various amounts and levels of complexity and sensitivity of the documents.

b) *Short terms must apply only when exists a proven necessity for information in an emergency regime, such as when the information is needed to protect the life or freedom of a person.*

Article 16 of the Law no. 982/2000 provides that:

(1) The requested information, documents, shall be made available to the requester from the moment they will be available to be submitted, but not later than 15 working days from the registration date of the request for access to information.
(2) The information provision deadline may be extended by 5 working days by the head of the public institution if:
a) the request refers to a very large amount of information which needs to select it;
b) are necessary additional consultations to satisfy the request.
(3) The author of the request shall be informed about any extension of the term for the provision of information and about its motives 5 days before the expiry of the initial deadline.

For a greater clarity of procedure, in the spirit of Principle 25 a), Para 1 from above should be modified to link the moment of start of the period and not with the registration of the request (operation under full control of the public authority, unverifiable in the situation of sending some requests to a distance), but with its receipt. This way the requester would have a clear understanding of the moment of receipt (by the chosen confirmation modality), while the public authority won't be able to delay the reply by delaying the registration of request. Also, is necessary to complete Art.16 in the sense of introduction of a new emergency deadline when the situation needs it, in conformity with the requirements of Principle 25 b).

Regarding the internal control, Art.22 of the Law no. 982/2000 provides, also, clear and short terms:

(1) In case when the person considers that his legitimate rights or interests related to access to information were affected, he can appeal the actions or inaction of the data provider in front of his management and/or the hierarchically superior body of the provider in a 30 day term from the date when he did find out or ought to find out about the violation.
(2) The management of the data provider and/or its hierarchically superior body shall review the appeals of the requesters for information in a 5 working day term and shall inform mandatorily the petitioner on the result of the review in 3 working days.
(3) *Intimations, by which are appealed the actions or inaction of the organisations which don't have their superior bodies, are addressed directly to the competent administrative court.*

The judiciary control also has clear and short terms provided by Law in conformity with Art.23 Para2 of the Law no. 982/2008: *the intimation of the court shall be done in a month term from the date of receipt of the reply from the data provider or, in case of no reply received, from the date when it ought to be received. If the requester of information did previously appeal the actions of the data provider extra judicially, the one month term starts from the date of disclosure of the reply to the management of the data provider and/or its hierarchically superior body or, if no reply was received, from the date when it ought to be received.*

Conclusion: *This principle is partially followed. The national legislation provides short and*

clear deadlines, but doesn't provide emergency deadlines when a situation requires it.

Principle 26: Right to review the decision to not-disclose information

a) A requester has the to a quick and cheap review of the refusal to disclose information or matters related to the request by an independent authority;

Note: A refusal may be implicit or tacit. Taxes, deadlines and the format represent aspects which are the object of review of an independent authority.

b) The independent authority must have due competency and resources to ensure the efficient review, including the full access to relevant information, even if it is classified;

c) A person must have the right to obtain an independent and effective review of all relevant aspects by a competent court or tribunal.

d) In case when a court pronounces a decision in conformity with which the nondisclosure of information is justified, it should make public in writing the specific factual grounds and its legal analysis, except some extraordinary circumstances and in conformity with Principle 3.

Law no. 982/2000 in Art.21 provides the procedure to appeal a refusal to disclose official information:

(1) A person who considers himself affected in a right or legitimate interest by the data provider may appeal its actions extra judicially, as well as directly to the competent administrative court.

(2) The person, also, may appeal for the protection of his legitimate rights and interests to the parliamentary advocate.

(3) A person who considers himself affected in a right or legitimate interest may appeal any action or inaction of the person responsible for the receipt and review of requests for access to information, but especially regarding:

a) ungrounded refusal to receive and register the request;
b) refusal to provide free access to the public registers which are at the disposal of the data provider;
c) violation of terms and procedure to solve the request for access to information;
d) non-presentation or undue presentation of the requested information;
e) ungrounded refusal to submit the requested information;
f) ungrounded attribution of information to the category of information which contains state secrets, commercial secrets or category of other official information with limited accessibility;
g) ungrounded classification of some information;
h) setting a fine and an amount for it in relation with the provided information;
i) causing material and/or moral prejudice by the illegal actions of the data provider.

(4) When solving disputes on access to information, the competent bodies shall undertake measures to protect the rights of all persons whose interests may be affected by the disclosure of information, also assuring their participation to the process as a third party.

(5) *The court, when reviewing litigations on access to information, shall undertake all reasonable and sufficient measures of caution, including calling closed hearings, in order to avoid disclosure of information, the limited access to which may be justified.*"

The procedure is explained hereinafter and in Art.22 and 23 (cited previously) and corresponds to the requirements of Principle 26.

Conclusion: *At the legislative level this principle is followed.*

PART IV. JUDICIARY ASPECTS OF THE NATIONAL SECURITY AND THE RIGHT TO INFORMATION

Principle 27: Principle of overall court supervision

a) *Invoking national security can't be used only to undermine the fundamental right to a fair trial on behalf of a competent, independent and impartial tribunal, set by the Law;*
b) *When a public authority seeks to refuse disclosure of information based on a motive of national security within any legal procedures, a court must have the competence to review the information to find whether the information may be refused. The court shouldn't refuse the appeal without reviewing the information;*
   Note: In conformity with Principle 4 (d), the court shouldn't rely on summaries or declarations which only affirm the need to preserve the secret, without providing an evidential base for statements.
c) *The court must make sure that the requesting person may, as much as possible, now and challenge the statements of the Government in order not to disclose information;*
d) *The court must state on the legality and groundless of Government's statements and may order disclosure or compensatory measures suitable in case of a partial or full nondisclosure, including the rejection of accusations in criminal procedures.*
e) *The court must evaluate independently whether the authority did solidly invoke any motive of nondisclosure; the classification fact shouldn't be decisive for the nondisclosure of information. Similarly, the court must evaluate the nature of any prejudice invoked by the public authority, the chances for it to happen and the public interest for disclosure, in conformity with the standards provided by Principle 3.*

Should be mentioned the fact that this principle doesn't refer strictly to the appeal procedures for the refusal to disclose information or for classification (analyzed above), but to any kind of procedures where is incident information related to the national security, administrative, civil, criminal or of another kind. In general, the legislation of the Republic of Moldova doesn't provide such situations where the right to a fair trial would be restrained based on motives of national security.

Moreover, the courts and other judiciary bodies have the possibility to access classified information, to be able to realize in practice the requirements of Principle 27, based on a declaration of nondisclosure. Also, in conformity with Art.213 Para 5 of the Criminal Procedure Code: *defenders and other representatives, as well as other persons whom, in conformity with the criminal procedure norms, shall be presented to take act of or communicated in another way, data which represents state secret, shall submit a prior written declaration of nondisclosure of this data. In case when his defender or another, except the legal representative, refuses to provide such a declaration, he is deprived of the right to take part to the respective criminal process, while the other persons won't have access to the data which represents a state secret. The declaration of nondisclosure from the persons mentioned in this paragraph is taken by the person who carries out the criminal investigation or the court and is annexed to the respective criminal file. The obligation of nondisclosure assumed by the participants to the process doesn't prevent them to request the review of data representing a state secret in a closed court hearing.*

For a full transposition of Principle 27, but also of Principle 30, must be undertaken measures so than within any court proceedings, except the criminal ones, to have applied the same rule on the access of the persons involved into the procedure, as much as possible, to the classified information, in conformity with Principle 27 c). Regarding the rejection of the criminal charges in the absence of access to the secret information which stays at the basis of the accusation, that shall be done based on the right to a fair trial, provided by the European Convention for Human Rights, in Article 6, as well as by the legislation of the Republic of Moldova (see also Principle 29).

Conclusion: *This principle is partially transposed into the national legislation, since the access to classified information within judiciary procedures is limited.*

Principle 28: Public access to court trials

a) *Invoking national security can't serve as motive to undermine the fundamental right of the public to have access to court trials;*
b) *Court decisions – containing all the disposals of the court, including the main conclusions, evidence and legal motivations – must be made public, less when the interests of children below the age of 18 y.o. require it;*

Note: The international law doesn't allow for any derogation, based on national security motives, from the obligation to pronounce decisions in a public manner.

Don't have to be made public the records of the judiciary procedures with minors. Records of other judiciary procedures involving children must normally hide the name and other identification data for children below the age of 18 y.o..

c) *The public right of access to justice must include prompt public access to: a) the court motivations; ii) information on the existence and progress of reasons; iii) arguments brought in from of the court; iv) court hearings and trials; v) evidence within procedures in court, which are at the basis of a sentence, except when a derogation from this is justified in conformity with the present principles;*

Note: In a democratic society the international right on the requirements for a fair trial allow the courts to exclude from the hearing a part of or all the public from motives of national security, as well as morality, public order, in the interest of the private life of the parties or to avoid affecting the interests of justice, with the condition that these restrictions are in all cases necessary and proportionate.

d) *The public must have the opportunity to challenge any statement of the public authority that a restriction of public access to the judiciary procedures is strictly necessary based on national security motives;*
e) *When a court orders to restrict access to court proceedings, then must be made publically available the factual and legal motives of the decision, except the extraordinary circumstance, in conformity with Principle 3.*

Note: This principle doesn't seek to modify the existing Law of a state regarding preliminary proceedings to which the public, usually, doesn't have access. It applies only

when the court trial would allow in a different way the public access and the attempt to prevent access would rely on invoking the national security.

The public right to have access to court proceedings and materials derives from the importance of the access for the promotion of the (i) real and perceived fair character and impartiality of the court proceedings; (ii) corresponding and more honest behaviour of the parties, as well as (iii) consolidated fairness of the public comments.

In general, Principle 28 is followed, in the sense that there is public access to the court proceedings and court decisions. This may be restricted, in the criminal matter in conformity with Art.18 of the Criminal Procedure Code, which imposes the motivation in conformity with Principle 28 e):

(1) In all courts hearings are public, except cases provided by the present Article.

*(2) The access to the hearing room may be prohibited to mass-media or the public, by a motivated decision, during the whole trial or a part of the trial, in the interest to protect morality**, public order or national security,** when the interests of the minors or the protection of the private lives of parents in the trial require that, or in the extent considered strictly necessary by the court when, due to some special circumstances, the publicity could affect the interests of the court.*
(2^1) In the matter where the minor is a victim or witness, the court shall listen to his statements in a closed hearing.
(3) The trial of the matter in a closed court hearing must be grounded and done following all rules of the judiciary procedure.
(4) In all cases, the court decisions are pronounced in a public hearing.

In civil matters also Principle 28 is followed. Article 23 from the Civil Procedure Code sets the public character of the court hearings, as well as exceptions from this principle:

(1) In all courts, trial hearings are public. To the court hearing aren't admitted minors below the age of 16 y.o. if they are not cited as participants to the trial or witnesses.
(2) May be held closed hearings only in order to protect the information representing state secret, trade secret or another information the disclosure of which is prohibited by Law.
(3) The court may order re-trial of the matter in a secret hearing in order to prevent disclosure of some information which refers to private aspects of the life, which affect the honour, dignity or professional reputation or other circumstances which might prejudice the interests of the participants to the trial, public order or morality.
(4) The hearing may be declared secret for the whole trial or solely for some procedural actions.
(5) Regarding the review of the matter in a secret hearing, the court issues a motivated decision.
(6) The secret hearing is held in the presence of the participants to the trial, while in case of necessity it is assisted by the witness, expert, specialist and interpreter.
(7) The court undertakes the due measures in order to keep the state secret, trade secret, information on the private life of the person. The participants to the trial and other persons assisting to the procedural acts during which can be disclosed data representing such secrets are summoned on the liability for their disclosure.
(8) The trial of the matter in a secret hearing is done following all rules of civil procedure.

(9) The decisions of the secret hearing are pronounced in public.
(10) In case of the trial of the matter in closed hearing, may be issued to other people besides the parties copies of the decisions, expert reports or witness statements only with the permission given by the chair of the hearing.

Conclusion: *This principle is followed since the national legislation provides the public character of court hearings during criminal and civil matters.*

Principle 29: Access to information of the party in criminal matters

a) *The court can't prohibit a culprit to take part to his own trial based on motives of national security;*
b) *In no situation a sentence or deprivation of freedom can't be based on evidence which the culprit didn't have the possibility to learn and challenge;*
c) *In the interest of justice, public authorities must make available to the culprit and his defenders the charges against a person and any information necessary to ensure the right to a fair trial, regardless whether the information is classified, in conformity with Principles 3-6, 10, 27 and 28, including by the consideration of the public interest.*
d) *When a public authority refuses to disclose information necessary to provide a fair trial, the court must suspend or reject the charges.*

Note: Public authorities shouldn't rely on information in their benefit when they pretend the preservation of the secret, although they may decide upon keeping the secret of the information and supporting consequences.
Note: Principles 29 and 30 are included into these principles on the public access to information, taking into account the fact that the court reviews, as well as related disclosures in the context of court supervision, represent important means for public disclosure of information.

Principle 29 is followed, the culprit having access to secret information which stays at the basis of the charges, through the defender (see also the explanations from Principle 27). The full translation into practice of Principle 29 presumes the strict application of the right to a fair trial and of the presumption of innocence, provided by the criminal legislation of the Republic of Moldova. In this sense and for a unitary application of the Principle, would be useful to be issued by the Plenary of the Supreme Court of Justice of the Republic of Moldova a guiding decision on the criminal procedures involving secret information.

Conclusion: *At the legislative level this principle is followed*

Principle 30: Access to information of the party in civil matters

a) *All statements on the refusal of a public authority to disclose information in a civil matter must be subject to control in a manner which is in conformity with Principles 3-6, 10, 27 and 28, including by the consideration of the public interest.*

b) *Victims of the human rights violations have the right to remedies and effective repairing, including public disclosure of supported abuses. Public authorities can't refuse relevant information for their matter in a modality contrary to this right;*
c) *The public also has the right to information on severe violations of human rights and of the humanitarian law.*

Within procedures of appeal against the refusal to disclose information, the courts have full control over the statements of the public authorities (see also the explanations of Principle 3). But it is unclear whether such powers exist also regarding other types of civil litigations, in this regard being useful the issue by the Plenary of the Supreme Court of Justice of the Republic of Moldova of a guiding decision, to ensure the compliance with Principle 30.

Regarding the violations of the human rights, these can't represent state secret information, and there's no reason for their nondisclosure.

Conclusion: *At the legislative level this principle is followed.*

PART V. SUPERVISORY BODIES OF THE SECURITY SECTOR

The Resolution 1954 (2013) of the Parliamentary Assembly of the Council of Europe states, at a principle level, in Art.9.9: *public supervision bodies, empowered to supervise the activity of the security services must be independent from the executive and have relevant experience, serious competences and full access to the protected information.*

Principle 31: Setting up of independent supervisory bodies
States must set up, if not existing, independent supervisory bodies for the entities from the security sector, including their operations, regulations, policies, finance and administration. Such supervisory bodies must be independent institutionally, operationally and financially from the institutions they are mandated to supervise.

Taking into account also those presented at Principle 3 on the independent supervisory bodies, it results that these do exist (People's Advocate and Parliamentary Commission for the Control of ISS) but with limited power, through the perspective of requirements of Principles 32 – 36. Consequently is needed the modification of the legal framework on existing bodies or the creation of a new body which would answer to *Global Principles,* the decision belonging to the authorities.

Also is necessary to train the staff of the People's Advocate and create good practice at the level of this institution to exercise a real and efficient control over the abuses in the area of access to information in the sector of national security.

Conclusion: This principle is translated partially into the national legislation because although independent bodies exist, they have limited competences.

Principle 32: Unrestricted access to information necessary to fulfil the mandate

a) *The independent supervisory bodies must have legally guaranteed the right of access to all information needed to fulfil the mandate. There should be no restriction to access, regardless of the level of secrecy or confidentiality of information, after the fulfilling of some reasonable secured access conditions;*
b) *Information which the supervisory bodies must have access to include, but aren't limited with:*
    i) *All records, technologies and systems in the possession of the authorities of the security system, regardless the form or environment* [of storage] *or whether were created or not by that authority;*
    ii) *Physical localizations, objects and facilities, and*
    iii) *Information held by persons whom are considered relevant by the supervisory bodies for their supervisory positions.*
c) *Any obligation of the public staff to keep the secret or confidentiality shouldn't prevent them from offering information to the supervisory bodies. Disclosure of such information*

must not be considered a violation of the Law or contract obligations which impose protection of confidentiality.

Regarding the People's Advocate, he has, in conformity with Art.11 Letter k) of the Law no.52/2014, the right *to request and receive from public authorities, from people in accountable positions of all levels information, documents and materials necessary to fulfil his duties, including official information with limited access and information attributed to the state secret in the conditions of the Law*, being followed Principle 32.

The Commission for the Control of the ISS Activity has, in conformity with Art.28 of the Regulations of the Parliament, a limited access to state secret information:
(5) The sub-commission members have access to secret information, signing every separate time, an engagement to protect the confidentiality of the information representing state secret, carrying liability in conformity with the legislation.
(6) The sub-commission members may request, with the agreement of its chair, secret information and information on the current activity of I.S.S., except the information on operative activities of the service or identity of persons working under cover, being part of the registered staff or having specific mission which need nondisclosure of identity", Principle 32 being followed.

In case when is chosen the consolidation of the parliamentary control of the activity of information services, the Regulations of the Parliament should be modified to provide the possibility for the sub-commission members and its staff to have access to all the information provided by Principle 32. The Regulations of the Parliament or subsequent Regulations of the sub-commission (which must be public) shall be completed substantially to provide with maximum accuracy the procedures by which the parliamentary control is done, but also those which are to protect the state secret information. The sub-commission must have provided specialized auxiliary staff which would assist it in its activity, taking into account the fact that at every election process the sub-commission members may change.

Conclusion: *This principle is partially followed because the parliamentary sub-commission has a limited to classified information.*

Principle 33: Competences, resources and procedures necessary to provide access to information

a) *The independent supervisory bodies must have adequate legal powers to be able to access and to interpret any relevant information which they consider necessary to fulfil the mandate;*
   i) *These powers must include at least the right to question the current and past members of the executive power, and employees and contractors of the public authorities, to request and inspect relevant records and inspect locations and physical facilities;*

ii) *The independent supervisory bodies must, also receive the authority to hear such persons and records and take testimonies under oath or declarations from persons suspected of possessing information which is relevant to fulfil their mandate, with the full cooperation of the law enforcement agencies, when necessary.*

b) *The independent supervisory bodies, when processing information or testimonies, must take into consideration,* inter alia*, the relevant provisions of the right to private life, as well as protection against the self-incrimination and other requirements of a fair trial;*
c) *The independent supervisory bodies must have access to financial, technological and human resources necessary to allow the identifying, accessing and analysing information which is relevant to fulfil effectively their duties;*
d) *The Law must oblige the institutions of the security sector to provide the independent supervisory bodies with the cooperation the need to access a and interpret the information necessary to fulfil their duties;*
e) *The Law must oblige the institutions of the security sector to disclose to the independent supervisory bodies, from own initiative and on time, categories of information which the independent supervisory bodies found as being necessary to fulfil their mandate. This information must include, but not be limited to possible violations of the Law and of the human rights standards.*

The Law provides sufficient rights to the People's Advocate (Art.11 din Law no. 54/2014) which would be in conformity with the requirements of Principle 33: *in the exercise of his mandate, the People's Advocate has the right:*

a) *to be received in audience by the President of the Republic of Moldova, by the Chair of the Parliament and by the Prime Minister within the hours of hearing as well as outside them;*
b) *to be received in audience immediately and with no form of obstruction or delay by the heads and other persons in accountable positions at all levels of public authorities, institutions, organizations and enterprises, regardless of the type of property and legal organisational form, of police inspectorates and detention places within, of penitentiary institutions, criminal investigation isolators, military units, placement centres for immigrants or asylum seekers, of the institutions providing social, medical or psychiatric care, of special education re-education institutions or curative institutions and for the re-education of minors and other similar institutions;*
[...]
c) *to verify compliance and according exercising by public authorities, by organisations and enterprises, regardless the type of property and legal organisation form, by non-commercial organizations, by persons in accountable positions at all levels of their duties regarding the protection of the human rights and freedoms;*
[...]
d) *to act ex oficio in cases provided by Law;*
e) *to have free access to all public authorities, to assist to the meetings of their subdivisions, including meetings of their collegial bodies;*
f) *to have free and immediate access to institutions, organizations and enterprises, regardless of the type of ownership and legal organization form, to police inspectorates and detention places within, to penitentiary institutions, to criminal investigation*

isolators, to military units, to placement centres for immigrants or asylum seekers, to the institutions providing social, medical or psychiatric care, to the special education re-education institutions or curative institutions and for the re-education of minors and other similar institutions;

g) to have unlimited and immediate access, at any moment of the day, to any sector of the detention places, to any information on the treatment and conditions of detention of persons deprived of freedom;

h) to request and receive from public authorities, from people in accountable positions at all levels information, documents and materials necessary to exercise their duties, including official information with limited accessibility and information attributed to state secret in the conditions of the Law;

i) to invite for auditions and receive from people in accountable positions explanations and information necessary to reveal the circumstances of the reviewed case;

[...]

j) to have unlimited meetings and confidential discussions, without witnesses, and when necessary through an interpreter, with the person located in the places listed at Letter b), as well as any other person who, in his opinion, could provide useful information;

k) to request conclusions of the competent institutions regarding the protection of the human rights and freedoms in the case when there are sufficient grounds to suspect the infringement of the rights and freedoms guaranteed by the Constitution of the Republic of Moldova and by international treaties which the Republic of Moldova is party to;

[…]

Also, Art.23 of the Law no. 52/2014 provides that: *(1) when reviewing requests, in order to verify the presented facts, the People's Advocate has the right to request the involvement of authorities and people in accountable positions in order to organize the control of the circumstances which shall be elucidated. The control can't be given to the authority or person in an accountable position whose decisions, actions or inactions are challenged.*
(2) Persons in accountable positions at all levels are obliged to present to the People's Advocate all materials, documents and information requested in relation with the exercise of his duties in no more than 10 days from the date of request, if the request doesn't provide another term."

Still, for the People's Advocate to exercise these duties really and effectively in the area of access to information from the national security sector is necessary to ensure resources for this institution, from the financial, logistical and vocational perspectives.

On the other hand, regarding the Sub-commission for the Control of the ISS Activity, there's no public provision to explain its rights, needing, as well as for Principle 32, a serious review of the regulations which are at the basis of operation of this sub-commission, even if is chosen the set up of another control body.

Conclusion: *At the legislative level this principle is partially followed since the national legislation provides sufficient powers for the People's Advocate, fact which is not valid for the parliamentary sub-commission.*

Principle 34: Transparency of the independent supervisory bodies

A. Applicability of the legislation on access to information

The legislation on the exercise of the public right of access to information held by public authorities must apply to the independent supervisory bodies.

B. Reporting

(1) The independent supervisory bodies must be obliged legally to develop periodical reports and make these reports publically available. These reports must include, at least, information on the independent supervisory bodies in them, including on their mandate, composition, budget, performance and activities.

Note: These reports must contain, also, information on the mandate, structure, budget and general activities of any institution from the security area, information which is not made by default available to the public.

(2) The independent supervisory bodies must offer public versions of reports which refer to thematic and case studies and investigations and must also provide as much information as possible on matters of public interest, including on the areas listed at Principle 10;

(3) In the public reporting, the independent supervisory bodies must protect the rights of all stakeholders, including their right to private life;

(4) The independent supervisory bodies must offer institutions which are object of the supervision the opportunity to analyze, timely, any report which shall be made public to allow them raise objections regarding the inclusion of materials which might be classified. The final decision o what must be published shall stay with the supervisory body itself.

C. Availability and accessibility

(1) The legal basis of the supervisory bodies, including mandates and powers, must be publically available and easily and accessible.

(2) The independent supervisory bodies must develop mechanisms and facilities for illiterate persons, who speak the languages of minorities or who have sight or hearing impairments to access information about their activity;

(3) The independent supervisory bodies must offer a range of freely accessible mechanisms by which the public, including people form geographically remote areas, to be helped to get into contact with them and, in the case of the complaints processing bodies, to submit complaints or express concerns.

(4) The independent supervisory bodies must have mechanisms which would allow the effective protection of confidentiality of complaints and anonymity of the complainer.

Regarding Principle 34 A, the People's Advocate as well as the parliamentary sub-commission is abiding the legislation on access to official information. Regarding the sub-commission is necessary in the detailed regulations of its operation, which must be public and easily accessible, in conformity with Principle 34 C (1), to provide clear rules of access to information on its activity.

Also regarding Principle 34 B, the situation is similar: the People's Advocate has such obligations of transparency, while the parliamentary sub-commission operates in a regulatory

vacuum, at least at the public level. Regarding Principle 34 B (4), Law no. 52/2014 provides, in Art.23 Para3: *the People's Advocate applies all diligence to solve requests by conciliating parities and seeking mutually acceptable solutions. Conciliation may take place at any stage of review of the request and, at the request of the parties, may end up by signing a conciliation agreement. The conciliation of the parties may serve as ground to cease the process of review of the request*. Thus, although it doesn't provide expressly the provision of an opportunity to the controlled authorities to express an opinion before the publishing of a report, this procedure of conciliation may easily cover this obligation.

The People's Advocate also has an accessible legal base, while the access mechanisms of the public are, in general, in their turn, accessible. Article 19 of the Law on the organization and operation provides:*(2) Requests are submitted in person or by mail, fax, e-mail or another mean of disclosure. The request may be submitted also by a proxy of the person whose rights were infringed, by the nongovernmental organizations, trade unions and other representative organizations on his behalf.*
(3) The request on behalf of a person in detention, a person in the criminal investigation isolators, on behalf of militaries from the military units isn't subject to censorship and is sent by the administration of the respective institutions to the People's Advocate in a 24-hour period.
(4) Requests addressed to the People's Advocate are exempted of the stamp duty.
(5) The People's Advocate reviews also verbal requests, coming from the hearings organised less than once a month, in conformity with the regulations approved by the People's Advocate.

A special mention should be given to the provisions from Art.21 Para5 Letter e), which provides that the People's Advocate doesn't review a request submitted by a person declared incapable by a court decision. Or, these persons also may be victims of violations of some rights, including in the area of access to information from the area of national security, so that, regarding them, must be modified Law no. 52/2014 or created a good practice to intimate ex oficio the People's Advocate in such situations, starting eventually from the intimations of such persons, on foot of Art.22 Para 1 which provides that *in case when having the information on mass or severe violation of the human rights and freedoms, in cases of a special social importance or in the case when is necessary the defence of some persons who can't use on their own legal means of protection, the People's Advocate has the right to act ex oficio*.

Also, the People's Advocate has the obligation to keep confidential the complaints received, in conformity with Principle 34 C (4), based on Art.12 Para1 Letter c) of the Law no.52/2014.

Regarding the sub-commission, the intimation and confidentiality protection rules should be clearly detailed in the public operational regulations.

Conclusion: *This principle is partially translated into the national legislation, since there are regulations only for the institution of the People's Advocate, while the provisions regarding the mechanisms of the parliamentary sub-commission should be regulated more clearly.*

Principle 35. Measures for the protection of information administrated by supervisory bodies from the security sector

a) *The Law must impose independent supervisory bodies to implement all due measures to protect information in their possession.*
b) *Legislatives must have the power to decide whether i) members of legislative supervisory committees and ii) heads and members of the independent non-legislative bodies shall be subject to security control before being appointed.*
c) *When the security control is requested, it must be undertaken i) timely, ii) in conformity with some established principles, iii) without political partisanship or motivation and iv) as much as possible by an institution which isn't supervised by the entity whose members/staff are controlled.*
d) *In conformity with principles from PART VI and VII, the members or staff of the independent supervisory bodies who disclose classified or confidential matters in any other way besides normal reporting mechanisms of the body must be subject to the corresponding administrative, civil or criminal procedures.*

Regarding the sub-commission for the supervision of ISS, the requirements of Principle 35 must be found in the detailed and public regulations of its operations. In principle, there are limitations regarding the information processed by it in Art.28 of the Regulations of the Parliament, but these are too general to assess the extent of full compliance with Principle 35.

The People's Advocate has the obligation to protect the secret character of the processed information, on foot of Art.12 Para1 Letter b) of the Law no.52/2014.

Conclusion: *This principle is partially followed because is imposed the need for detailed and publically accessible regulations on the operations of the parliamentary sub-commission.*

Principle 36: The power of the legislative to make information public

The Legislative should have the power to disclose public information, including information without which the executive power supports a right to refuse disclosure based on national security motives, if it appreciates this as suitable, in conformity with procedures which must be established.

In the absence of some detailed and public regulations of the parliamentary sub-commission, Principle 36 isn't followed. Moreover, in conformity with Para 5 of Art.28 of the Regulations of the Parliament *"the members of the sub-commission have access to secret information, signing, in each separate case, an engagement to keep the confidentiality of information which represents a state secret, being liable in conformity with the legislation",* from where it results that, in principle, there's no power for the legislative to disclose public information refused from disclosure based on national security motives, besides the generally applicable rules. Thus, this power should be provided expressly in the new public regulations of the activity of the sub-commission.

Conclusion: *This principle isn't followed because are missing the detailed and publically accessible regulations on the powers of the parliamentary sub-commission.*

PART VI: INFORMATION OF A PUBLIC INTEREST DISCLOSED BY PUBLIC SERVANTS

Public staff (or **public servant**) is defined by *Global Principles* as *current and ex-employees, contractors or sub-contractors of public authorities, including in the sector of security. Public staff also includes persons employed by non-state entities which are held or controlled by the Government and which act as agents of the Government; and employees of private entities or other entities which perform public duties or services or operate significant public funds or benefits, but only regarding the performance of these functions, provision of services or use of public funds or benefits.*

A the general principle level, Resolution 1954 (2013) of the Parliamentary Assembly of the Council of Europe provides in Art.9.7: *a person who discloses wrongdoings in the public interest (whistle-blower) should be protected from any type of retaliation, provided he or she acted in good faith and followed applicable procedures.*.

Principle 37: Categories of illegal activities

Disclosure, by public servants, of information, even classified, which shows illegal activities which fit one of the following categories must be considered ''protected disclosure'', if it follows the conditions set by Principles 38-40. A protected disclosure may refer to an illegal activity which took place, takes place or shall take place.

a) Offences;
b) Violations of the human rights;
c) Violations of the international humanitarian law;
d) Corruption;
e) Health and public safety hazards;
f) Environmental hazards;
g) Abuse of a public position;
h) Judicial errors;
i) Bad administration or waste of resources;
j) Punishment for the disclosure of any abuses from the above categories; and
k) Deliberate concealment of any matter fitting in the above categories.

In conformity with Art.8 Para 5 of the Law no. 982/2000, *nobody can be punished for making public certain information with limited accessibility, if the disclosure of information doesn't affect and can't affect a legitimate interest related to the national security or if the public interest to know the information exceeds the prejudice which might be done by the disclosure of information*.

Moreover, Law no. 245/2008 provides in Art.8 that: (1) *Isn't attributed to state secret and can't be classified the information on:*

a) facts of violations of the human and citizen rights and freedoms;
b) the condition of the environment, quality of the food products and home appliances;
c) accidents, catastrophes, dangerous natural phenomena and other extraordinary events which affect the security of citizens;

d) the health condition of the population, its living standard, including nutrition, clothing, healthcare and social security, social-demographical indicators;

e)) the health condition of the persons holding high-ranked public positions;

f) facts of violation of the Law by public authorities and persons in accountable positions from within;

g) the real state of things in the area of education, culture, trade, agriculture and of public order.

Isn't attributed to state secret and can't be classified also other information in conformity with the national legislation and international treaties which the Republic of Moldova is party to.

(2) Is prohibited the classification of information in case when it could limit access to information of a public interest, could reflect negatively on the realization of the state and branch programs for the social-economic and cultural development or could retain competition among companies.

It results that such an information could be made public, even if it's secret, without a person to be held liable for this.

Regarding the information which refers to corruption, the legal framework is completed by the provisions of the frame Regulations on the Whistle-blowers, approved by Government Decision no.707/2013. [17]

Still, taking into account that this decision refers only to the disclosure of information regarding acts of corruption, while the protection of protected disclosures is broader and envisages an obviously sensitive area, it is recommended for similar regulations to be adopted also for disclosures with a broader context provided by Principle 37. It would need to overtake the requirements imposed by Principles 37-44, presented hereinafter. Moreover, the regulation on the whistle-blowers, in the greatest part, doesn't follow the same principles, so that their urgent review is needed, taking into account the fact that Principle 37 includes disclosures of acts and facts of corruption. Ideally should be adopted a single Law, applicable to all these types of disclosures, regarding facts of corruption, or classified or confidential information and the correlation of its provisions, through the perspective of the below principles, with the criminal, civil and administrative legislation.

Conclusion: *This principle is partially translated into the national legislation because there are no regulations on protection in case of disclosure in the area of national security.*

Principle 38: Grounds, motivation and proof for disclosure of information showing illegal activities

a) The Law must protect from repressions, defined in conformity with Principle 41, against public servants who disclose information showing illegal activities, regardless whether the information is classified or confidential in any other way, as long as, at the moment of disclosure:

[17] Published in the Official Monitor of RM no.198-204 from 13.09.2013.

(i) the person making the disclosure had reasonable motives to believe that the disclosed information shall prove illegal activities which fit one of the categories provided by Principle 37, and

(ii) the disclosure follows the conditions provided by Principles 38-40

b) The motivation for a protected disclosure is irrelevant except situations when is proven the fact that it was known that the information is untrue;

c) A person who makes a protected disclosure shouldn't be asked to bring evidence to support or to support the burden of proof in relation to the disclosure.

Conclusion: *This principle isn't found in the national legislation.*

Principle 39: Procedures i for protected disclosure and reactions to this disclosure

A. Internal disclosure

The Law must put in the tasks of public authorities the obligation to regulate internal procedures and appoint persons whom the protected disclosures shall be addressed to.

B. Disclosures made to independent supervisory bodies

(1) The states must also set up or identify independent bodies to receive and investigate protected disclosures. Such bodies must be independent institutionally and operationally from the security sector and from other authorities from where the disclosures are made, including the executive.

(2) Public servants must be authorised to do protected disclosures to independent supervisory bodies or to any other body competent to investigate the matter without being obliged first to make the internal disclosure.

(3) The Law must guarantee that the independent supervisory bodies have access to all relevant information and provided them with the due powers of investigation which would ensure access. Such powers must include those of hearing and the power to request a testimony to be under oath or affirmation.

C. Obligations of the internal bodies and of the independent supervisory bodies which are disclosing/receiving disclosures

If a person makes a protected disclosure, as defined by Principle 37, internally or to an independent supervisory body, the body which disclosure is addressed to must be obliged to:

1. *Investigate the violation of the claimed law and to undertake prompt measures in order to solve the matter in a period of time provided by law or, after consulting the person who has made the disclosure, to refer him to a body which is authorised and competent to investigate it;*
2. *Protect the identity of the public servant who seeks to make confidential disclosures; anonymous disclosures must be examined in substance;*
3. *Protect the disclosed information and the fact that disclosure was made except and within the limits of the situation in which additional disclosure of information is needed to remedy the violations of Law; and*
4. *Notify the person making the disclosure about the evolution and ending of an investigation and, as much as possible, on measures taken or recommendations made.*

Conclusion: *This principle isn't found in the national legislation.*

Principle 40: Protection of public disclosure

The Law must protect from repressions (as defined in Principle 41) related to disclosures to the public of the information on the violations of Law (as defined by Principle 37, is the disclosure fulfils the following criteria:

a) *1. The person who has made an internal disclosure and/or to an independent supervisory body of the same or of the very similar information and:*
   i) *The body to which disclosure was made did refuse to or didn't investigate disclosure effectively, in conformity with the applicable international standards; or*
   ii) *The person didn't receive a reasonable and suitable remedy, in a reasonable period set by Law.*

   OR

   2. The person did reasonably consider that there's a significant risk for her, in case of an internal disclosure and/or to an independent supervisory body, the evidence to be destroyed or hidden, to be influenced by a witness or to be subject to repression herself or a third party;

   OR

   3. There's no internal or independent supervisory body which the disclosure would be made to:

   OR

   4 Disclosure refers to an act or omission which represented a severe and imminent risk which would endanger the life, health or safety of a person or of the environment.

   AND

b) *The person who has made the disclosure did unveil as much information as was reasonably necessary to show the illegal activity*

Note: If, during a process of disclosure of information which denotes an illegal activity a person discloses also documents which are not relevant to prove the illegal activities, the person should be still protected from repressions, except the case when the prejudice of disclosure prevails over any public interest for disclosure.

AND

c) *The person who has made the disclosure did reasonably consider that the public interest in the disclosure of information exceeded any prejudice brought to the public interest by disclosure.*

Note: The test "has reasonably considered " is a mixed objective-subjective test. The person, in fact, must have thought (subjectively) and the though should have been reasonable for him or her to proceed so (objectively). If challenged, the person might need to defend the reasonable character of his thought and, in the end, to be at the discretion of an independent court or tribunal to find whether this test was fulfilled, so that disclosure would become protectable.

Conclusion: *This principle isn't found in the national legislation.*

Principle 41: Protection against repressions for disclosures of information which proves illegal activities

A. Civil and criminal immunity protected disclosure

A person who has made a disclosure, in conformity with Principles 37-40, must not be subject to:

(1) Criminal proceedings, including, but not limited to criminal investigation for disclosure of classified or confidential information; or

(2) Civil procedures related to disclosure of classified or confidential information, including but not limited to attempts to obtain damages or defamation procedures;

(3)

B. Prohibition of other forms of repressions

1. The Law must prohibit the repression of any person who has made, is suspected of making or could make disclosures in conformity with Principles 37-40.

2. The prohibited forms of repressions include, but are not limited to:

a) Administrative measures or sanctions, including but not limited to: warning letters, investigations with a sanctioning character, retrograding, transfer, change of powers, non-promotion, firing, actions which may lead or intent to bring prejudice to the reputation of a person or the suspension or revocation of a security certificate:

b) Physical or emotional injuries or harassment; or

c) Threats with any from above.

3. Actions undertaken against other persons but the one who made the disclosure can, in certain circumstances, represent prohibited repressions.

C. Investigation of repressions by an independent supervisory body and by court authorities

1. Any person must have the right to intimate an independent supervisory body and/or a judicial authority on any measure of repression or threat with repressions, in relation with a protected disclosure.

2. The independent supervisory bodies must investigate an intimation on repressions or threat with repressions. Such bodies should have the possibility to start an investigation in the absence of an intimation on repressions.

3. The independent supervisory bodies must have the powers and resources to investigate effectively any alleged repressions, including the power to hear persons and obtain documents and hear witnesses under oath or affirmation.

4. The independent supervisory bodies must undertake all efforts to make sure the procedures on alleged repressions are fair and in conformity with the fair trial standards.

5. The independent supervisory bodies must have the authority to request the respective public authorities to adopt remediating or restoring measures, including but not limited to re-employment; re-appointment; and/or payment of legal fees and other reasonable costs, the retroactive payment of the salary and of other benefits, travelling costs and/or compensatory damages.

6. *The independent supervisory bodies must have the authority to order the public authority to refrain from punitive sanctions.*
7. *Such bodies must finalize the investigation in a reasonable period of time, set by the Law.*
8. *Such bodies must notify relevant persons at least regarding the finalization of the investigation and, as much as possible, on the measures taken and recommendations made;*
9. *People may challenge in court the decision of the independent supervisory body, in conformity with which the actions following disclosure do not represent repressions or repairing or recovering measures.*

D. Burden of proof

If a public authority undertakes a measure against any person, the authority has the task to prove that the measure wasn't related to the disclosure.

E. Non-waiver of rights and remedies

Can't be waived or limited the rights and remedies provided by Principles 37-40 by no form of agreement, public policy, employment form or condition, including by no pre-trial arbitrage agreement. Anny attempt to waive or limit the rights and remedies must be considered null.

Conclusion: *This principle can't be found in the national legislation.*

Principle 42: Encouraging and facilitating protected disclosures

The states must encourage public servants to make protected disclosure. In order to facilitate such disclosures, the states must request from all public authorities to issued regulations which shall implement into practice Principles 37-42.
Note: These regulations should provide, at least: (1) recommendations on the rights and/or responsibilities to disclose illegal activities, (2) types of information which must or may be disclosed, (3) procedures necessary to make such disclosures; and (4) protection provided by Law.

Conclusion: *This principle can't be found in the national legislation.*

Principle 43: Defending public interest for public servants

a) *Every time a public servant is subject to criminal or civil procedures or administrative sanctions, in relation with the disclosure of information which isn't otherwise protected by these Principles, the Law must provide the possibility for these to defend invoking public interest, if the public interest for disclosure of the respective information doesn't exceed the public interest for non-disclosure.*

Note: This principle applies to all disclosures of information which aren't protected yet, due to the fact that the information doesn't fit one of the categories mentioned in Principle 37, or due to the fact that disclosure contains information which fits into one of the categories mentioned in Principle 37, but wasn't done in conformity with the procedures described on Principles 38-40.

b) In order to decide whether the public interest for disclosure exceeds the public interest for non-disclosure, the criminal investigation and court authorities must take into consideration:

i) Whether the extent of the disclosure was reasonably necessary for disclosure of information of a public interest;

ii) The extent and risk of prejudice to the public interest caused by disclosure;

iii) Whether the person had reasonable motives to believe that disclosure would have been in the public interest;

iv) Whether the person did try to make a protected disclosure through internal procedures and/or to an independent supervisory body, and/or to the public, in conformity with procedures described in Principles 38-40; and

v) The existence of some urgent circumstances which justify disclosure.

Note: Any law which provides criminal punishments for an unauthorised disclosure of information should be in correspondence with Principle 46 (b). This principle doesn't seek to limit any right to free expression already available to public servants any other protection guaranteed in conformity with Principles 37 - 42 or 46.

Conclusion: *This principle isn't found in the national legislation.*

PART VII. LIMITS RELATED TO SANCTIONNING MEASURES OR TO RESTRAIN TO DISCLOSE INFORMATIONI TO THE PUBLIC

Principle 44: Protection against sanctions for reasonable disclosure, done in good faith by the communication officers

Persons with duties to reply to requests for information from the public must not be sanctioned for the disclosure of information about which they reasonably and in good faith though they can disclose in conformity with the Law.

Law no. 158/ 2008 on the public position and the status of public servant[18] provides, in Art.22(e), that *the public servant is obliged to protect, in conformity with the law, the state secret, as well as the confidentiality in relation with the facts, information or documents which he sees while exercising the public position, except information considered of a public interest*. From this provision results that there's no obligation to refuse disclosure of classified information when we speak about information of a public interest. Still, this aspect should be expressly provided in Law no. 982/2000.

Conclusion: *This principle is followed at the legislative level.*

Principle 45: Sanctions for the destruction or refusal to disclose information

a) *Public staff must be subject to sanctions for the intended destruction or modification of information, with the aim to deny access to it.*
b) *If an institution or an independent body did order disclosure of information and the information isn't disclosed in a reasonable time, the official and/or public authority responsible for non-disclosure must be subject to some corresponding sanctions, except situations in which was filed an appeal in conformity with the legal procedures.*

The Criminal Code of the Republic of Moldova provides a specific offence for the intended violation of the legislation on access to information, in Art.180: *The intended violation by a person in an accountable position of the legal procedure of ensuring and realizing the right of access to information, violation which did cause damages in considerable proportion to the rights and interests protected by the Law, of the person who did request the information regarding healthcare of the population, public safety, environmental protection, is punished with a fine from 150 to 300 conventional units with (or without) deprivation of the right to hold certain positions or exercise a certain activity for a period for up to 3 years.*

Also, the Contraventions Code of the Republic of Moldova provides sanctions for the violation of the secret regime within public authorities as well as other legal entities (Art.365[1]), as well as

[18] Published in the Official Monitor of RM no. 230-232 from 23.12.2008.

for the ungrounded classification/declassification of information (Art.365[2]). These transpose the requirements imposed by Principle 45.

Conclusion: *This principle is followed at the legislative level*.

Principle 46: Limitations regarding criminal punishments for disclosure of information by public servants

a) *Public disclosure of information, on behalf of a public servant, even if unprotected by PART IV, must not be subject of criminal sanctions, although might be subject to administrative sanctions, such as the loss of security certificates or even dismissal.*
b) *If the Law imposes some criminal sanctions for unauthorised disclosure of information to the public or to people with the aim for the information to be made public, the following conditions must apply:*
    i) *Criminal sanctions must apply to the disclosure of some restrained categories of information which are clearly set by Law;*

Note: If the national legislation provides for categories de information the disclosure of which could make the object of some criminal sanctions, these must be similar whit the following regarding the specifics and impact on the national security: technological data on nuclear weapons, sources of secret information, codes and methods; diplomatic codes, identities of undercover agents and intellectual property, where the state has property interests, as well as knowledge which might prejudice the national security.

    ii) *Disclosure must produce a real and identifiable risk of causing an important damage;*
    iii) *Any criminal sanction, as provided by Law and applied, must be proportionate to the created damage; and*
    iv) *The person should be able to defend the public interest, as provided by Principle 43.*

The Criminal Code of the Republic of Moldova sanctions the disclosure of state secret information by the public staff in Art.344, Principle 46 being incident from the perspective of letter b:

(1) Disclosure of information representing state secret by a person to whom this information was entrusted or became known in relation with his work or jib, if it doesn't represent treason of the home country or espionage, is punished by a fine amounting from 200 to 600 conventional units or prison for up to 4 years, in both cases with the deprivation of the right to hold certain positions or exercise certain activity for a term for up to 5 years.

(2) The same action followed by severe consequences is punished with prison from 3 to 7 years with the deprivation of the right to hold certain positions or exercise a certain activity for a term from 2 to 5 years."

The criminal code doesn't provide expressly the circumstances from Principle 46 b), so that in principle, the criminal court wouldn't be able to apply them in order not to sanction criminally the person making the disclosure. Still, the accused may invoke the defence of the public interest, on foot of Art.8 Para 5 of the Law no. 982/2000, while the court may take into consideration the

requirements of Principle 46 b) at the individualizing of the punishment. In order to clarify this situation is needed a modification of Art.344, in the sense of removal of criminal liability for disclosure of a public interest.

Conclusion: *This principle is partially followed since the national legislation doesn't contain provisions on the exclusion of criminal liability in case of disclosures in the public interest.*

Principle 47: Protection against sanctions for the possession and dissemination of classified information by persons who aren't public servants

a) *A person who isn't a public servant can't be sanctioned for receiving, possessing or disclosure to the public of classified information.*
b) *A person who isn't a public servant can't be subject to accusations of conspiracy or other offences based on the fact that he sought and found Information.*

Note: This principle seeks to prevent the criminal liability for the procurement or reproduction of information. However, this principle doesn't have as aim the prevention of criminal investigation of an individual for committing other offences, such as theft or blackmail, committed while seeking for, or obtaining the information.

Note: Disclosures of third parties work like an important correction for the general over-secrecy.

The Criminal Code of the Republic of Moldova doesn't sanction holding or transmitting classified information by other persons except those with powers in the areas. Regarding offences of treason and espionage, their area of application is relatively restrained, being circumstantial to some specific aims, which don't include the simple obtaining of classified information. Consequently, in general, Principle 47 is followed. Still, it is necessary to train the judiciary bodies for the accurate application of these provisions, in the light of the *Global Principles*, so that abuses would be prevented.

Conclusion: *This principle is followed at the legislative level*.

Principle 48: Protection of sources

No person who's not a public servant must not be obliged to disclose a confidential source or unpublished materials in an investigation on the unauthorised disclosure of information by the press or public.
Note: This principle refers only to investigations on the unauthorised disclosure of information, not to other offences.

The Resolution 1954 (2013) of the Parliamentary Assembly of the Council of Europe also underlines the importance of the Principle of protection of sources, regarding reporters in p.11

recalling the Recommendation no. R (2000) 7 of the Committee of Ministers on the rights of the reporters not to disclose their sources of information, the Assembly reiterates that the following measures shouldn't be applied if their aim is to circumvent the right of the reporters not to disclose information which would identify a source:
11.1 orders of intercept or actions related to the communications or correspondence of the reporters or their employers;
11.2. orders of supervision or actions related to reporters, their contacts or their employers;
11.3. search or confiscation orders or actions regarding the domiciles or premises, property or correspondence or the reporters or of their employers, or personal data related to their professional activity".

Article 13 of the Law no.64/2010 on the freedom of expression provides[19] that:
(1) Mass-media and any person carrying out an activity with a reporter's characteristics of collection, receipt and distribution of information to the public, as well as the person who collaborates with these, who did obtain the information from a source, have the right not to disclose the identity of the source or any information which might lead to the identification of the source.
(2) The person who did distribute publically the information obtained from confidential sources can't be obliged to disclose the identity of the source within a civil or contravention trial.
(3) The refusal of the person to disclose the source of information doesn't exempt him from the other guarantees enjoyed by the defendant in a court trial.
(4) Within a criminal trial, the criminal investigation body or the court, in the conditions of the Law, may oblige the person to disclose the source of information if are cumulatively met the following conditions:
a) the criminal file envisages specifically severe or exceptionally severe offences;
b) disclosure of the source is absolutely necessary for the criminal investigation;
c) were exhausted all possibilities to identify the source of information by other means.

The deontological code of the reporters from the Republic of Moldova provides, in Art.3.1 and 3.2 the protection of sources: *3.1 The reporter protects the identity of sources, including in front of a court, public prosecutors, police officers and other law enforcement bodies. The protection of the professional secret and confidentiality of sources is in a equal extent a right and an obligation of the reporter.*
3.2 The protection of sources is provided only in those cases when disclosure of their identity endangers their life, safety or professional activity.

That is why, to follow Principle 49, should be introduced a guarantee in the criminal legislation (Criminal procedure code). Even in the absence of such a legislative modification, the protection of sources should produce by the application with priority of Art.10 of the European Convention of Human Rights. In this sense would be useful an explanation on behalf of the Plenary of the Supreme Court of Justice of the Republic of Moldova.

Conclusion: *This principle is followed at the legislative level.*

[19] Published in the Official Monitor of RM no.117-118 from 09.07.2010.

Principle 49: Prior prevention

a) Prior prevention of publishing in the interest of protection of national security must be prohibited.

Note: Prior preventions are orders of the judiciary bodies or other state bodies prohibiting the publishing of specific materials already in the possession of a person who is not a public servant.

b) If the information was made available to the public, by any means, legal or not, any attempt to stop the subsequent publishing of information in the form which is already in the public area is presumably invalid.

Note: By the term "generally available " is understood that information was disseminated on a quite broad scale, so that there are no specific measures which could be undertaken to keep information secret.

The legislation of the Republic of Moldova doesn't provide direct possibility for prior prevention of publishing of classified information. Regarding information which was already brought to public knowledge, it shall be mentioned that Law no. 245/2008 provides as ground for declassification, in Art.18 Para 1 Letter b) *change of objective circumstances, following which the further protection of certain information attributed to state secret becomes inappropriate*. Or, bringing to public knowledge represents exactly such a change of objective circumstances, so that any attempt to prevent the publishing of information can't have any more the grounds in its secret character. Consequently, Principle 49 is followed.

Conclusion: *This principle is followed at the legislative level.*

PART VIII. FINAL PRINCIPLE

Principle 50: The relationship between these principles and other standards

No provision of these principles should be interpreted as restraining or limiting any right to information recognised according to international, regional or national regulations and standards, or any norm of the internal or international law which would provide a greater protection for disclosure made by public staff or other people.

The translation into practice of this principle presumes that the *Global Principles* can't be interpreted as basis to restrict the right to access to information or protect disclosure in the public interest on foot of Art.3 Para 2 and/or Art.4 Para 2 of the Law no.982/2000. Also, this principle imposes any modification of regulations which would be undertaken by the state authorities to put the national legislation into correspondence with the *Global Principles* to have as and/or result the broadening of the right of access to official information from the area of national security and protection of those making protected disclosure, and not their limitation.

CONCLUSIONS AND RECOMMEDATIONS

This report aims to analyse the compatibility of the national legal framework with the provisions of the *Global Principles on the right to information and national security*. These principles, based on good international practices, contain the guarantees needed to provide the right to information in the area of national security. Practices existing in the RM in this area, as well as the degree of implementation of the current legislation weren't addressed within this research.

Following the analysis of the national legal framework in the area of access to information and protection of national security we did find that the provisions enshrined by these Principles can be partially found in the legislation of the Republic of Moldova. At the same time, some national provisions shall be reviewed and completed to ensure the effective exercise of the right to information in this area.

PART I: GENERAL PRINCIPLES

Principle 1: Right to information

Although the legislation RM provides, in principle, access for anyone to official information, it is recommendable the area of requesters of official information to be broadened. In this context, shall be extended the list of requesters of official information, including foreign citizens /stateless persons with no permanent domicile on the territory of RM and legal entities. This adjustment shall ensure the application of provisions of Article 10 of the European Convention for Human Rights.

The national legislation provides also the list of suppliers of data of a public interest. However, it is recommended for the definition of "public authorities" to be broadened at the national level to be in correspondence with the Principles and to provide a better functioning of the private contractors in the area of national security.

The obligation to disclose information at request or ex oficio is enshrined at the legislative level. Still, is recommended the adoption of some regulations which would detail the modality of enforcement for this obligation of disclosure ex oficio of the information from the area of national security.

Principle 2: Application of these principles

The national security is a broad and vaguely formulated concept in the national legislation. From this motive is imposed a clarification and a consolidated approach to the limitation of access to information of a public interest, based on national security motives. This can be realized either by a more accurate definition of the national security or by the limitation of the concept.

Principle 3: Condition for the limitation of the right to information, based on national security motives

The national legislation provides the triple test conditions, while the legal regulations in the area of secret information are clear and accessible. Also, the categories of information excepted from disclosure, based on a national security motive, are restrictively provided by the Law. However a

careful analysis is recommended on behalf of the state authorities for all the secondary regulations (bylaws) as well as the adoption of measures to make public all regulations containing information provided by Principle 10.

Although the extrajudicial remedy doesn't represent any guaranties against the abuse of the current regulation, the judiciary control meets the conditions of independence, has the vocation to be complete, and is accessible and partially efficient. Consequently, to provide full efficiency to the procedure of judicial review of the refusal to disclose information based on national security motives, the legal framework should be modified to include also declassification of information among the solutions pronounced by a court.

Principle 4: The task of the public authorities to find the legitimacy of any restriction

The national legislation sets the task on the public authority to find the legitimacy of restrictions, as well as the obligation to motivate the refusal of access to information.

Principle 5: No exception for no public authority

No public authority isn't exempted from the obligation to disclose information in conformity with the national provisions.

Principle 6: Access to information of the supervisory bodies

At the legislative level, the supervisory institutions, such as the court instances and the People's Advocate, have access to all relevant information to fulfil their mandates, regardless of the secrecy level. However, shall be reviewed the normative provisions on access of the Sub-Commission for the Control of the ISS Activity to relevant information to fulfil its duties in order to exclude the limitations provided by Law.

Principle 7: Resources

In order to follow this principle, the state authorities must make sure to allocate the due resources to protect the right to information, in conformity with the *Global Principles.*

Principle 8: State of emergency

This principle is reflected in the national legislation, including by providing additional guarantees on the restrain of the rights of citizens during the state of emergency. However, it is recommended to define the categories of information to which the access wouldn't be restricted during the state of emergency.

PART II. INFORMATION WHICH MAY BE UNDISCLOSED BASED ON NATIONAL SECURITY MOTIVES AND INFORMATION WHICH MUST BE DISCLOSED

Principle 9: Information which may be legitimately undisclosed

The national legislation contains an exhaustive list of information which may be attributed to the state secret. However, it is recommended when the refusal of disclosure of information is due to

its secret character, to clearly specify whether this disclosure prejudices the state security or its interests.

Principle 10: Categories of information with an increased presumption or major interest in favour of disclosure

The list provided by Principle 10 can't be fully found in the national legislation, which is more restrained. Still, in general, the internal Law covers the same type of information for which is presumed the existence of a supreme interest in favour of disclosure.

PART III. RULES ON CLASSIFICATION AND DECLASSIFICATION OF INFORMATIONI

Principle 11: The obligation to declare motives for the classification of information

The legislation of RM provides a formal procedure for classification. However, it is recommended for the legal provisions and/or subsequent internal regulations (bylaws) on classification to be modified to clarify the classification procedure. A solution would be the existence of a written decision/declaration, mandatory to classify an information, decision which would cover elements provided by Principle 11. The content of these decisions should be communicated, as possible, to the requesters of classified information, as motivation for the refusal to disclose those requested.

Principle 12: Public access to the classification rules

Although public authorities are obliged to undertake measures to provide the public participation to the decision-making process, is necessary the regulation of public participation to the process of adoption/review of written procedures and standards on classification, as well as clarification of the access to detailed registers of the departments.

Principle 13: Authority to classify

The classification process produces through registers of information, while the national legislation sets certain categories of persons who can approve them. However, it is hard to estimate whether p. c) of this principle is realized in practice.

Principle 14: Facilitation of internal appeals against classification

At the national level there are regulations on a general procedure for appeal against decisions to classify information, but aren't known any special provisions for the public staff, including the one affiliated to the security sector. That is why, would be welcome the introduction of a procedure similar to the one on the whistle-blower, on the internal appeals against improper classification.

Principle 15: Obligation to store, administrate and preserve national security information

The national legislation provides detailed conditions on the storage and administration of the classified information. However, isn't provided the obligation of the public authorities to keep public the lists of issued documents. So that is necessary the modification of the Law no.245/2008 to include such an obligation and of the Law no.982/2000 to include also classified documents included in the public lists of issued documents.

Principle 16: Time limits for the classification period

The formal procedure of declassification is provided by the national legislation. However, the Law shall be modified in the sense to introduce the obligation to review classified information or refusals to disclose classified information.

Moreover, information may stay classified for an unlimited period. In these conditions is necessary the modification of Art.13 of the Law no. 245/2008 to make it in correspondence with Principle 16 c) and d). The extension of the maximum period of classification may be done only in exceptional circumstances by another decision-maker and with a clear indication of the new period of classification.

Principle 17: Declassification procedures

Although the national legislation sets the authorities with declassification powers, it doesn't provide their obligation to analyse the opportunity of declassification of information of public interest from the area of national security and doesn't specify whether after the expiry of the classification term declassification is produced automatically.

Thus, Law no.245/2008 shall be modified, in the sense of including an obligation for the authorities with declassification powers to identify actively and analyze the opportunity of priority declassification of information of a public interest from the area of national security, as well as specify the conditions automatic declassification produces in.

PART III B. RULES ON THE ADMINISTRATION OF REQUESTS FOR INFORMATION

Principle 18: Obligation to take into consideration the request, even if the information was classified

The national legislation provides the general obligation to analyse any request for information. However, it is necessary for this Principle to be promoted in practice, by the corresponding training of the servants tasked with the analysis of the requests for official information.

Principle 19: Obligation to confirm or infirm

The national legislation provides the form of the refusal to disclose information. Still, for a complete translation the Decision of the Plenary of the Supreme Court of Justice of the Republic of Moldova no.1/2007 should be supplemented in the sense of introducing the obligation for the motives for which a simple confirmation or denial of existence of information would endanger a distinct category of information.

Principle 20: Obligation to put in writing the motives for the refusal

The national legislation provides the obligation to motivate the refusal in writing.

Principle 21: Obligation to disclose parts of documents

Principle 21 isn't found in the legislation of the Republic of Moldova. Thus, is recommended the modification of Law no. 982/2000 to include also this obligation to recover or restore the information, in the case when information can't be localized, although it should have been preserved, collected or produced.

Principle 22: Obligation to disclose parts of documents

The national legislation provides access to parts of classified documents, as long as a document which contains classified parts and unclassified parts shall carry the corresponding labels on each part.

Principle 23: Obligation to identify the undisclosed information

This principle can't be found in Law no. 982/2000 except indirectly, by the obligation to motivate the refusal for disclosure.

Principle 24: Obligation to provide information in the available format

The legislation of RM places it in the task of the requester to include in the request for information the acceptable modality to receive information.

Principle 25: Deadlines to answer to requests for information

For a better clarity of procedure, the national legislation should be modified to ling the moment of start for the term not with the registration of the request, but with its receipt. Also, is necessary the introduction of an urgency term when the situation requires it.

Principle 26: Right to review the decision of nondisclosure of information

The national legislation provides the procedure of appeal against a refusal to disclose official information.

PART IV. LEGAL ASPECTS OF THE NATIONAL SECURITY AND THE RIGHT TO INFORMATION

Principle 27: Principle of general judiciary supervision

The access to classified information within the judiciary procedures is limited. Shall be taken measures so that within any judiciary procedures, besides the criminal ones, to apply the same rule on access of people involved into the procedure, as much as possible, to classified information.

Principle 28: Public access to court trials

The national legislation provides the public character of the court trials within criminal and civil processes.

Principle 29: Access to information of a party within criminal matters

In this sense and for a sole application of the Principle, shall be useful the issue by the Plenary of the Supreme Court of Justice of the Republic of Moldova of a guiding decision on criminal procedures which involve classified information.

Principle 30: Access to information of a party within civil matters

The national legislation provides the access to information of a party in civil matters.

PART V. SUPERVISORY BODIES FOR THE SECURITY SECTOR

Principle 31: Establishment of independent supervisory bodies

Although the independent bodies exist, they have limited competences. Consequently, is needed whether the modification of the legal frame on the existing bodies or the establishment of a new body.

Also, is necessary the training of staff of the People's Advocate and the creation of good practices at the level of this institution to exercise a real and efficient control on the abuses in the area of access to information in the sector of national security.

Principle 32: Unrestricted access to information necessary to fulfil the mandate

In case when is chosen the consolidation of the parliamentary control of the activity of information (intelligence) services, then the Regulations of the Parliament must be modified to provide the possibility for the members of the sub-commission and its staff to have access to all information provided by Principle 32.

Principle 33: Competences, resources and procedures necessary to ensure access to information

In conformity with the national legislation, the People's Advocate has sufficient rights to ensure access to information. Still, is necessary to ensure resources for this institution, from the financial as well as logistical perspective.

On the other hand, regarding the sub-commission for the control of the ISS activity, there's no public provision which would explain its rights. Is necessary the review of regulations which are at the basis of activity of this commission.

Principle 34: Transparency of the independent supervisory bodies

There are regulations on the transparency of the institution of the People's Advocate while the provisions on the mechanisms of the parliamentary sub-commission aren't clear enough. In this context, the rules to intimate and keep the confidentiality shall be clearly detailed in the public operational regulations.

Principle 35. Measures for the protection of information administrated by the supervisory bodies from the security sector

Regarding the sub-commission for the supervision of ISS, the requirements of Principle 35 must be found in detailed and public regulations of its operation.

Principle 36: The authority of the legislative in making the information public

This power should be provided in the new public regulations of the sub-commission activity.

PART VI. DISCLOSURE IN THE PUBLIC INTEREST MADE BY PUBLIC SERVANTS

Principle 37: Categories of illegal activities

In the national legislation are missing regulations on the protection in case of disclosures in the area of national security.

Principle 38: Grounds, motivation and proof for disclosure of information which reveals illegal activities

This principle isn't found in the national legislation.

Principle 39: Procedures for protected disclosure and reactions to these

This principle isn't found in the national legislation.

Principle 40: Protection of public disclosure

This principle isn't found in the national legislation.

Principle 41: Protection against repressions for disclosure of information which proves illegal activities

This principle isn't found in the national legislation.

Principle 42: Encouraging and facilitating protected disclosures

This principle isn't found in the national legislation.

Principle 43: Defence of the public interest for public servants

This principle isn't found in the national legislation.

PART VII. LIMITS REGARDING SANCTIONING OR RESTRAIN MEASURES OF THE DISCLOSURE OF PUBLIC INFORMATION

Principle 44: Protection against sanctions for reasonable disclosure made in good faith by the communication officers

This principle is followed at the legislative level.

Principle 45: Sanctions for the destruction or refusal to disclose information

This principle is followed at the legislative level.

Principle 46: Limitations regarding criminal punishments for disclosure of information by public servants

Is necessary a modification of Art.344 CP, in the sense of elimination of criminal liability for disclosure of a public interest.

Principle 47: Protection against sanctions for possession and dissemination of classified information by persons who are not public servants

The Criminal Code of the Republic of Moldova sanctions only the possession or transmission of classified information by people with powers in the area.

Principle 48: Protection of sources

The national legislation provides protection of sources. However, to comply with Principle 49, should be introduced a guarantee in the criminal legislation (Criminal procedure code).

Principle 49: Prior prevention

The legislation Republic of Moldova doesn't provide directly the possibility for a prior prevention to publish classified information, but provides as grounds for declassification the change of objective circumstances, following which the further protection of certain information attributed to the secret becomes inappropriate.

PART VIII. FINAL PRINCIPLE

Principle 50: The relationship between these principles and other standards

Changes in national legislation, to be taken for harmonization with the Global Principles will aim at, and /or result in widening the right of access to official information on national security and to protection of those who make protected disclosures, and not limit such rights.