MEMORANDUM

on

The Law On Classified Information of The Former Yugoslav Republic of Macedonia

by

ARTICLE 19
Global Campaign for Free Expression

London
May 2004

I. *Introduction*

This Memorandum provides an analysis of the Law on Classified Information (Law), adopted by the Parliament of the Former Yugoslav Republic of Macedonia (Republic of Macedonia) in February 2004. The analysis, which addresses the degree of consistency of the Law with international standards relating to the right of freedom of information, is based on an unofficial translation of the Law.[1]

The Law contains some positive features, principal amongst which are a robust harm test applicable to all but one classification category and a mechanism which would declassify certain information of public importance. At the same time, we are concerned that the Law may undermine the freedom of information regime currently being considered by the Macedonian authorities in the form of the Law on Free Access to Information (the FOI Law). This is a particular threat given the climate of secrecy which still pertains in the Republic of Macedonia. Indeed, we question why there appears to be no attempt to coordinate the development of these two laws – the Law makes no reference to the FOI Law – given their proximity in terms both of subject matter and time of adoption. We note, in this regard, that various potential problems posed by the Law, from the point of view of freedom of expression, could

[1] ARTICLE 19 takes no responsibility for the accuracy of the translation or for comments based on mistaken or misleading translation.

be mitigated to a considerable degree by the addition of a provision in this Law, or in the FOI Law, to the effect that conflicts between the two laws are to be resolved in favour of the FOI Law.

In addition to the fundamental concern just noted, we have a number of specific concerns with the Law which we detail below. These include that: some of its classification categories are defined in terms which are unduly broad; it does not adequately specify who will be responsible for classifying certain types of information; reviews of classification decisions will not be sufficiently frequent and may not be adequately objective; and no protection is provided for whistleblowers.

We recognise that the Law has come into force only very recently, but we are of the view that it is of the greatest importance to bring it into line with international human rights standards in this area. This Memorandum analyses the Law with reference to those standards, and in its discussion of particular problematic provisions, it makes recommendations regarding how they should be amended to conform fully to the standards.

II. *International and Constitutional Standards*

II.A International Guarantees of Freedom of Expression

Freedom of information is of fundamental importance. During its first session in 1946, the United Nations General Assembly adopted Resolution 59(1) which stated:

> Freedom of information is a fundamental human right and…the touchstone of all the freedoms to which the UN is consecrated.[2]

In ensuing international human rights instruments, freedom of information was not set out separately but as part of the fundamental right of freedom of expression, which includes the right to seek, receive and impart information. The *Universal Declaration of Human Rights* (UDHR)[3] is generally considered to be the flagship statement of international human rights. Parts of it, including Article 19 guaranteeing the right to freedom of expression and information, are binding on all States as a matter of customary international law. Article 19 states:

> Everyone has the right to freedom of opinion and expression; this right includes the right to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

The *International Covenant on Civil and Political Rights* (ICCPR),[4] a legally binding treaty to which the Republic of Macedonia became a State Party in 1994, guarantees (in its Article 19) the right to freedom of opinion and expression in terms very similar to those of the UDHR. The *European Convention on Human Rights* (ECHR),[5] to which the Republic of Macedonia became a State Party in 1997, guarantees the right to freedom of expression and information at Article 10. Freedom of expression is also protected by the two other regional human rights instruments, at Article 9 of the

[2] 14 December 1946.
[3] UN General Assembly Resolution 217A(III), adopted 10 December 1948.
[4] UN General Assembly Resolution 2200A(XXI), adopted 16 December 1966, in force 23 March 1976.
[5] Adopted 4 November 1950, in force 3 September 1953.

African Charter on Human and Peoples' Rights[6] and at Article 13 of the *American Convention on Human Rights*.[7]

These guarantees allow for some restrictions on freedom of expression and information but only where these are prescribed by law, pursue a legitimate aim and are necessary in a democratic society to protect that aim. Of particular relevance to the analysis below is the fact that the international instruments themselves specify, *exhaustively*, which aims are to count as legitimate. As provided in the ECHR, these aims include protection of national security, territorial integrity or public safety, prevention of disorder or crime, the protection of health or morals, protection of the reputation or rights of others, prevention of the disclosure of information received in confidence, and maintenance of the authority and impartiality of the judiciary. The ICCPR list is somewhat shorter, not explicitly including maintenance of the authority and impartiality of the judiciary or referring to territorial integrity.

II.B Standards Relating to Freedom of Information

Numerous official statements have been made to the effect that the right to freedom of expression includes a right to access information held by public authorities. For example, the UN Special Rapporteur on Freedom of Opinion and Expression has frequently noted that the right to freedom of expression includes the right to access information held by public authorities. He first broached this topic in 1995 and has included commentary on it in many of his annual reports since 1997. Typical is the statement in his 1998 Annual Report:

> [T]he right to seek, receive and impart information imposes a positive obligation on States to ensure access to information, particularly with regard to information held by Government in all types of storage and retrieval systems….[8]

In November 1999, the three special mandates on freedom of expression – the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression – came together for the first time under the auspices of ARTICLE 19. They adopted a Joint Declaration which included the following statement:

> Implicit in freedom of expression is the public's right to open access to information and to know what governments are doing on their behalf, without which truth would languish and people's participation in government would remain fragmented.[9]

Within Europe, the Committee of Ministers of the Council of Europe recently adopted a Recommendation on Access to Official Documents.[10] Principle III of that Recommendation states:

---

[6] Adopted 26 June 1981, in force 21 October 1986.
[7] Adopted 22 November 1969, in force 18 July 1978.
[8] Report of the Special Rapporteur, *Promotion and protection of the right to freedom of opinion and expression*, UN Doc. E/CN.4/1998/40, 28 January 1998, para. 14. This view was welcomed by the UN Human Rights Commission. See Resolution 1998/42, 17 April 1998, para. 2.
[9] 26 November 1999.
[10] Recommendation No R (2000)2 of the Committee of Ministers to Member States on access to official information, adopted 21 February 2002.

> Member states should guarantee the right of everyone to have access, on request, to official documents held by public authorities. This principle should apply without discrimination on any ground, including that of national origin.

The European Union has also taken steps in recent years to give practical legal effect to the right to information. In May 2001, the European Parliament and the Council adopted a regulation on access to European Parliament, Council and Commission documents.[11] The preamble, which provides the rationale for the Regulation, states in part:

> Openness enables citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective and accountable to the citizen in a democratic system. Openness contributes to strengthening the principles of democracy and respect for fundamental rights….

The purpose of the Regulation is "to ensure the widest possible access to documents".[12]

Both other regional systems for the protection of human rights have also recognised the right to freedom of information. In October 2000, the Inter-American Commission on Human Rights approved the Inter-American Declaration of Principles on Freedom of Expression,[13] the most comprehensive official document to date on freedom of expression in the Inter-American system. The Principles unequivocally recognise freedom of information, including the right to access information held by the State, both as an aspect of freedom of expression and as a fundamental right on its own:

> 4. Access to information held by the state is a fundamental right of every individual. States have obligations to guarantee the full exercise of this right. This principle allows only exceptional limitations that must be previously established by law in case of a real and imminent danger that threatens national security in democratic societies.

A recent *Declaration of Principles on Freedom of Expression in Africa*, adopted by the African Commission on Human and Peoples' Rights, also recognises this key right.[14]

In 1999, ARTICLE 19 elaborated a set of standards on freedom of information, *The Public's Right to Know: Principles on Freedom of Information Legislation* (Article 19 Principles).[15] These Principles, which set out nine key standards on freedom of information, have been endorsed by, among others, the UN Special Rapporteur on Freedom of Opinion and Expression.[16] Principle 1, the Principle of Maximum Disclosure, stipulates: "The principle of maximum disclosure establishes a presumption that all information held by public bodies should be subject to disclosure and that this presumption may be overcome only in very limited circumstances".

---

[11] Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.
[12] *Ibid.*, Article 1(a).
[13] 108th Regular Session, 19 October 2000.
[14] Adopted at its 32nd Session, 17-23 October 2002. See Principle IV.
[15] (London, June 1999).
[16] Report of the Special Rapporteur, *Promotion and protection of the right to freedom of opinion and expression*, UN Doc. E/CN.4/2000/63, 18 January 2000, para. 43.

These international developments find their parallel in the passage or preparation of freedom of information legislation in countries in every region of the world. In the Republic of Macedonia itself, the FOI Law is currently in the process of being developed, for introduction to Parliament in the near future. Most States in Europe currently have freedom of information legislation on the books. Freedom of information laws or codes have been passed in Asia: for example, in Hong Kong, Japan, the Philippines, South Korea and Thailand. Similar developments are taking place in Africa and South America.

II.C Constitutional Guarantees

The right of access to information is recognised by Article 16 of the Constitution of the Republic of Macedonia, which states, in part:

> The freedom of speech, public address, public information and the establishment of institutions for public information is guaranteed.
> Free access to information and the freedom of reception and transmission of information are guaranteed.

III. *Analysis of the Law*

III.1 Basic Outline

Article 6 of the Law sets out the categories of information subject to classification, while Articles 8 and 10 establish the circumstances under which information falling within these categories may be classified and at what level of classification. Article 9, in conjunction with some relevant provisions scattered in later Articles, sets out who shall classify information, while Article 19 sets out time periods during which materials must be "examined" to determine if their classification status will continue or not.

Other Articles govern: (1) classified information received from foreign countries and international organisations; (2) measures – "administrative, physical, computing and industrial security, and security of people" – for protecting classified information; (3) the issuing of security certificates enabling certificate-holders to obtain access to classified materials, as well as principles governing the duration of such certificates; (4) the establishment and functioning of the Directorate, which is responsible for the enforcement of international and national standards relating to classification, which coordinates the classification of information and its exchange, and which ensures the protection of classified information; and (5) the imposition of sanctions for certain prohibited acts.

III.2 Relationship with the Freedom of Information Law

Despite the close connection between their subject matters, the Law makes no reference to the FOI Law which, as mentioned above, is likely soon to be put before Parliament. However, Article 7(2) of the FOI Law, as it existed in November 2003, provided that information that "has been declared as classified State, military, official or business information" is not subject to disclosure.

We recommended that the FOI Law be redrafted to include a provision to the effect that, in the event of inconsistencies between it and other information-related

legislation, including the classification Law, the FOI Law prevails. This is effectively the reverse of the Article 7(2) rule just noted. We also recommended that the FOI Law include a general public interest override, which was absent from the version we analysed.

In a number of countries, FOI laws supersede classification laws, so that the classification system is effectively an internal information management system. When a request for information is made under an FOI law, the mere fact of classification does not mean that the request will be denied. Rather, a request may be denied only if it falls within the scope of an exception specifically listed in the FOI law. If the regime of exceptions in a freedom of information law is comprehensive, as we recommend, it should not be permitted to be extended by other laws.[17] A system like this protects as secret all information the disclosure of which would harm a legitimate interest. At the same time, it avoids a situation whereby other laws, not drafted with openness in mind, extend the regime of secrecy beyond cases of harm to legitimate interests.

If the FOI Law remains as it is, the classification Law effectively operates as an additional set of exceptions to the right of access. This obviously has important implications in terms of the right to access information held by public bodies, and requires the classification Law to control classification far more tightly than if the FOI Law were to override it.

As noted, our primary recommendation is that the rule stated in Article 7(2) of the November version of the FOI Law be reversed, by a provision to this effect in either the FOI Law or the classification Law. In our present analysis of the classification Law, however, we proceed on the assumption that that Law is not relevantly constrained by the FOI Law, and that classification effectively means that the public will not be able to access the relevant information.

Recommendation:

- In case of inconsistency between the classification Law and the FOI Law, the latter should dominate.
- The Law should make explicit reference to the FOI Law and it should be drafted in such a way as to take that law into account.

III.3 Categories of Classifiable Information

Article 6 of the Law provides that information falling within the following categories may be classified: "public security; defence; foreign affairs; security, intelligence and counter-intelligence activities of the organs of the State government of the Republic of Macedonia; systems, appliances, projects and plans of importance to the public security, defence[,] foreign affairs; scientific research and technological, economic and financial affairs of importance to the Republic of Macedonia".

Analysis

As we have explained, any restriction on access to public information must serve a legitimate aim. While most of the aims provided for in Article 6 are recognised as legitimate in international law, the last one – "scientific research and technological,

[17] See the ARTICLE 19 Principles, Principle 8.

economic and financial affairs of importance to the Republic of Macedonia" – is too broadly defined. It is doubtful whether international law recognises the legitimacy of protecting national commercial and technological interests. Even if it does, however, the specification here sets an unacceptably low standard of mere "importance to the Republic". It therefore envisages restricting access to a much wider range of information than could, even on a broad interpretation, be appropriate under international law.

Recommendation:

- The final aim provided for in Article 6 should be deleted. If it is retained, it should at least be restricted to scientific research and technological, economic and financial affairs of *critical* importance to the Republic of Macedonia.

III.4 The Classification Scheme

Article 8 provides for four classification levels:

- Information is classified as a *State secret* if its unauthorised disclosure "would jeopardise and cause *irreparable damage to the vital interests* of the Republic of Macedonia";
- Information is classified as *highly confidential* if (1) it is "created by the state organs, organs of the units of the local government and other institutions", (2) it is "of importance to the public security, defence, internal affairs and security and intelligence activities of the organs of the state government of the Republic of Macedonia", and (3) its unauthorised disclosure "*would cause extremely serious damage to the vital interests* of the Republic of Macedonia";
- Information is classified as *confidential* if conditions (1) and (2) just above are satisfied, and if unauthorised disclosure of such information "*would cause serious damage to the important interests* of the Republic of Macedonia";
- Information is classified as *internal* if its unauthorised disclosure "*would cause damage to* activities of the state organs, organs of the units of the local government, and other institutions which are of importance to the public security, defence, internal affairs and security and intelligence activities of the organs of the state government of the Republic of Macedonia".

In addition to these provisions, Article 10 appears to add yet another classification category. It provides that information "which is not for public use, and whose disclosure would reduce the efficiency of the activities of the state organs shall be assigned *for limited use only*". [All emphases above added]

Analysis

We note, to being with, the positive fact that all the classification categories other than the "for limited use" category are conditioned by strong harm tests; in these cases, only information whose disclosure *would* cause harm – varying in degrees as between the different classification levels – may be classified and hence withheld from the public. The requirement of a causal link between the release of such information and the occurrence of harm (indicated by the term "would"), and the generally high degree of harm required ("irreparable", "extremely serious", "serious"), is to be welcomed.

Despite this, there are substantial shortcomings with the regime, which need to be addressed to bring it into line with international human rights standards. First, three of the four sub-Articles clearly fail to require that the harm contemplated by the

disclosure of information relate to specific legitimate interests recognised under international law. In particular, in the first two sub-Articles, the harm need only relate to the "vital interests of the Republic" while in the third, the harm need only relate to the "important interests of the Republic". (The fourth sub-Article, as we note below, also arguably has this failing.)

As noted above, restrictions on the right to information are permissible only if they serve the legitimate aims delineated in the applicable international instruments. By contrast, in referring only to the vague notion of 'interests of the Republic', these sub-Articles leave it up to the discretion of those who make classification decisions to determine for themselves what these interests are when deciding whether or not to classify particular information. In a country historically characterised by a culture of secrecy, many interests not recognised in international law may be found by particular decision-makers to be "vital" or "important" interests of the Republic. According wide discretion in these matters will have the predictable result that much information will be classified which should not be.

It is true that two of these sub-Articles (but not the first one) do mention legitimate interests, stipulating that the information must be important to public security, defence, and so on. However, there is no direct link between the requirement of harm and these specific legitimate interests; instead, the harm requirement relates simply to a "vital" or "important" interest of the Republic. These sub-Articles should be redrafted to provide for classification only where harm directly threatens the legitimate interests listed.[18]

The fourth sub-Article is slightly different in nature, conditioning classification on harm to the activities of State bodies "which are of importance to the public security, defense, internal affairs and security and intelligence activities". It is possible that this is a question of translation. However, as the sub-Article reads in English, this could cover anything deemed to be damaging either to any body doing important work in the area of defence, etc., or to the activities of these bodies which are important to defence, etc. In both cases, this deviates from international standards which require the harm to relate directly to a legitimate aim (rather than to a body working in this area or even to the aim-related activities of that body).

Second, based on a literal reading of the Law's text, it is possible that the categories of highly confidential, confidential and internal would apply to information created (and possessed) by private institutions as well as to information created by public institutions. We acknowledge that our interpretation on this delicate point may simply be the result of shortcomings in the translation, and that the intent behind the Law is in no way to include private institutions generally within its scope. It is worth pointing out, however, that it would be quite appropriate (and would not, in any event, be

[18] We note additionally that all but the first sub-Article refer to information which is important to "internal affairs" of various institutions, without specifying what such internal affairs are. While information relating to some internal affairs of some governmental and other bodies (for example, information relating to the process of deliberation with respect to important matters of policy) may legitimately be classified, other such information (for example, information about internal corruption, about hiring and promotion procedures, and so on) is clearly of high public interest and should not be subject to classification.

workable) to require private institutions which are not working in a contractual relationship with government institutions to classification information.

Third, the "for limited use only" category is grossly overbroad. The term "not for public use" is not defined and the Law gives no guidance as to who is to make, or how to make, the judgment of what information is for public use and what is not. According unlimited discretion on this basic determination to persons who may have incentives to keep material out of public reach is a recipe for undermining the right to freedom of information. Moreover, the notion of "reduc[ing] the efficiency of the activities of the state organs" is both undefined and extremely broad. For example, information about fraud in the procurement process, about the salaries of highly-paid public employees or about violations of constitutional protections by law enforcement officials could cause embarrassment or worse to State organs with the potential effect, at least in the short run, of reducing their efficiency. This information is of great public interest and should never be withheld from the public.

Moreover, while the other classification categories are subject to obligatory review for re- or de-classification (see below), the category of "for limited use only" has no such review period. It is, therefore, entirely possible that once information is classified as "for limited use only", it may remain in this category indefinitely.[19]

Recommendations:

- The criteria for classifying information in Article 8 should require the prescribed harm to relate directly to the legitimate interests listed rather than to vague notions such as the interests of the Republic or the activities of public bodies.
- The Law should be amended to clarify that information created by and in the exclusive control of private institutions which are not in pertinent contractual relations with public bodies should not be subject to classification. [SEE COMMENT ABOVE]
- The "for limited use only" classification category should be removed from the Law.

III.5 The Public Interest Override

Article 20 creates, in effect, a means by which the classification of information will be annulled. It provides: "Information which is assigned a certain level of classification shall not be considered as classified information if it covers a criminal act, exceeds or abuses the authority or any other illegal act or procedure".

Analysis

This provision is welcome, recognising as it does that certain information is of sufficient public interest that its classification should be overridden. In effect, this is a public interest override to the power to classify, albeit limited in scope to the public interest categories listed, namely criminal acts, abuse of authority or other illegal actions.

[19] While Article 43 provides that a security check is not required for access to "limited use only" information, the Law does not indicate when, and under what circumstances, access to such information may be granted or refused.

Welcome as this provision is, it does not go far enough. In our view, *whenever the public interest in disclosure outweighs the potential harm from disclosure of classified information, the information should be subject to disclosure*. For example, a risk of serious harm to the environment or to public safety should also be grounds for overriding classification. A general public interest override is a crucial element in any information management system, playing a key role in ensuring that information of importance reaches the public.[20]

It is important to note, in this regard, that the FOI Law does not at present contain a public interest override and, as noted above, does not provide for access to classified information. This renders a public interest override in the classification law all the more important. In light of the recognition in the Law that certain public interests will outweigh any "harm-based" need to withhold information from public view, we recommend the expansion of Article 20 to effectively declassify any information where the harm resulting from its disclosure is outweighed by the public interest in having access to the information.

Recommendation:

- Article 20 should be expanded so that it contains a general public interest override provision.

III.6 Persons Responsible for Classifying Material

Article 9 provides that a number of different senior officials may classify information as a State secret. These include the President of the Republic, the President of the Parliament, the President of the Government, the President of the Constitutional Court, the President of the Supreme Court, ministers, the public prosecutor, the Chief of Headquarters of the Army, the Director of the Intelligence Agency, the Director of the Directorate and persons empowered by written consent by any of these persons.

The final sentence of Article 9 provides: "If regulated by law, international agreement or other regulation, persons from those acts shall assign classified information with level 'state secret'".

Article 7 provides: "The authorised person referred to in art. 9 of this law assign[s] the level of classification of information" and, immediately thereafter, lists the four levels of classification. But, as just noted, Article 9, by terms, is quite explicitly restricted to the "state secret" category. Moreover, nowhere else in the Law is there any indication of which individuals will be responsible for classifying information for any of the other classification categories. Article 11 refers to a "creator" of a level of classification and Article 12 provides that such creator must indicate the level of classification of a classified document in a visible place. Some other articles also refer to the creator but we have been unable to find any specification of which persons are responsible for classifying information, other than for the State secret category.

Analysis

We acknowledge that, in the original, it may be clear that the combination of Articles 7 and 9 imply, or say outright, that the persons designated in Article 9 are in fact responsible for classification of materials at all classification levels. However, we

[20] See the ARTICLE 19 Principles, Principle 4.

repeat that, at least in our English translation, the Law simply does not appear to specify who will classify information into categories other than that of State secret. We base our analysis below on the assumption that the Law fails to make this specification.

We note first that the Law is not clear as to the meaning of "creator". Article 12, for example, refers to "the creator of the classified information". Article 14 provides: "The creator changes the level of classification with his/her written consent …". These passages imply that the term "creator" refers to the person who *creates the classification category* and not to the person who creates *the information*. By contrast, however, Article 18 provides, in part: "The creator *of the information* specifies a time period or event until which the information can not be reclassified or declassified" (emphasis supplied). According to this reference, the "creator" is the person who creates the information. Despite this ambiguity, we are informed that the term "creator" refers to the creator of the information, and we proceed on that basis in our analysis below.[21]

The failure to specify those persons responsible for classifying information for any of the classification categories other than State secrets is an extremely serious shortcoming in the Law. Lacking any indication to the contrary, the Law would appear to leave it open to the full discretion of any officials in public bodies (and "other institutions") to make classifications or to appoint persons to make classifications on their behalf. As a result, the potential for abuse in the classification of information as highly confidential, highly confidential or internal or limited, is great. Indeed, it is not difficult to imagine that virtually all information of public importance and interest would run the material risk of being classified by one or another unnamed official.[22] This situation is exacerbated, moreover, by the fact that reviews of classification decisions are infrequent, and are made by the same person who makes the initial classification decision (see below).

The Law also fails to impose any qualifications on those with the power to classify. Article 62 does provide that the Directorate "trains the users of classified information, as well as the interested organs, organisations and individuals". It is not clear what the topic of such training would be, but the general tenor of the duties imposed on the Directorate suggests that this entity is principally devoted to the *protection* of information. There is, therefore, some basis to doubt that the training referred to here would include the protection of freedom of information.

The open-ended nature of the closing sentence of Article 9 is also problematic. According to that sentence, any person so designated by any "law, international agreement or other regulation" may classify information as a State secret, without the

[21] The situation is complicated by Article 9, which provides that certain persons are empowered to classify certain information as "state secret". It is quite clear that many, if not all, of these persons will not be the persons who were the creators of the information. This, then, suggests that the "creator" of information may not be the person who does the initial classification of the information he or she created, which appears inconsistent with the above (for how could the creator set the duration of a classification which he or she did not create, or indeed change that classification).

[22] Standing in sharp contrast is, for example, the system in the United States, according to which original classification authority may be exercised only by the President and Agency heads/officials designated by the President. While delegation is permissible, it must be limited to the minimum needed to administer the classification system.

Law in any way limiting this power. The effect is that despite the relatively rigorous definition of 'state secret' in this Law, any other law, agreement or even regulation may employ much weaker, or permissive, terms for classifying information as a State secret. The effect is to grant extremely wide powers outside of the remit of the Law to classify information as a State secret, potentially seriously diluting that category of classification, otherwise the most restrictive level.

Recommendations:

- Strict limits should be placed on who may classify information. This power should be restricted to a limited class of persons for whom it is necessary, for functional reasons, to be able to classify, and who are highly qualified and have received appropriate training.
- Decisions to classify should be open to independent review.
- The Law should clarify which persons are able to make classification decisions with respect to categories other than State secrets.
- The final sentence of Article 9 should be removed; the Law should be the sole source of authority for classifying information as a State secret.

III.7 Changing Classification/Declassification

Articles 14 and 17 provide that only the creator (or "another empowered person") may change the classification level of given information and, in particular, may declassify information. According to Article 13, this rule will not apply only where the creator cannot be determined or has "ceased to exist". Further, Article 16 provides that information automatically loses its classification (1) on a date specified in the document; (2) with the advent of a certain event specified in the document; (3) with the expiry of a specified time period; or (4) upon declassification.[23]

Article 18 provides that the creator determines a maximum period or event before the expiration or occurrence of which classified information must be re- or declassified, which period cannot exceed 10 years "unless the information needs longer protection determined with this or other Law". Article 19 specifies time limits within which information classified at the different levels is to be reviewed "in order to assess the need of further keeping of the classification". The time limits are: 10 years, for the "state secret" classification; five years for the "highly confidential" classification; three years for the "confidential" classification; and two years for the "internal" classification. No time limit is specified for the highly problematic category of "limited use only". There appears to be a conflict between these articles, inasmuch as Article 18 envisages the possibility of extending a ban on re-classification or de-classification review beyond 10 years if the information "needs longer protection", whereas Article 19 appears to impose a firm deadline of no longer than 10 years for such review.

Analysis

The re- and declassification schemes are seriously flawed. In the first place, the fact that only the creator (except in exceptional circumstances) can revisit classification decisions is inappropriate. There may be a natural, if mistaken, tendency of the person who originally found reason to restrict access to information to defend that decision

[23] Each of these methods appears to be controlled by the creator.

by maintaining the same classification.[24] Moreover, the fact that the same person revisits the classification decision will work to entrench decisions made with the intention to perpetuate inappropriate secrecy; only an effective and objective review process, involving fresh reassessments of classification decisions by unbiased persons, can be effective in reversing such trends. Accordingly, we recommend that the review process involve, in principle, the revisiting of particular classification decisions by qualified persons other than the person who took the original classification decision.[25]

Additionally, our view is that the time limits for review of classification decisions, at least for categories of State secret and highly confidential information, are too long. We note, for instance, that the Hungarian classification law provides for review every three years and the Bulgarian law every two years; we recommend a similar timeframe here. We note that this does not mean that the information will necessarily be re- or declassified, merely that its classification will be reviewed to assess whether or not it is still appropriate.

More fundamentally problematic, however, is the "catch-all" provision in Article 18 which at least *appears* to allow the period of review for re- or de-classification to extend beyond 10 years if such information "needs longer protection [as] determined with this or other Law". This provision has the effect of seriously undermining the system of review of classification whenever any other law provides that the information needs to be classified for a longer period of time. As noted above, we are of the view that 10 years is already too long a period for reviewing classification and we recommend that this catch-all be removed.

Finally, in the event that the "for limited use" category is retained, classifications of this level should also be subject to regular review.

Recommendations:

- Review of classified information for re- or declassification should be done by qualified persons other than the original creator of the classification category.
- The time limits for review of State secret and highly confidential information should be shortened.
- The catch-all provision in Article 18 should be removed.
- The "for limited used" category, if retained, should be subject to re- or declassification review on a regular basis.

III.8 Whistleblowers

To combat the prevailing culture of secrecy and to help expose wrongdoing, the Law should provide protection to whistleblowers who release classified information as long as they act in good faith and in the reasonable belief that the information was

[24] As noted above, it is unclear whether the term 'creator' refers to the creator of the information or to the creator of the classification. Regardless, re-classification and de-classification decisions should be taken by qualified persons other than those who made the original classification decisions – whoever these latter might be.

[25] The weaknesses in the classification scheme which we detail here and below point up the vital need for a provision *in the FOI Law* creating a right of review, by an independent body, of denials of requests for information based on the claim that the information is classified: part and parcel of such review should be an inquiry into whether the information had been appropriately classified in the first place.

substantially true and disclosed evidence of wrongdoing. Wrongdoing for these purposes should include the commission of a criminal offence, failure to comply with a legal obligation, a miscarriage of justice, corruption or dishonesty, or serious maladministration regarding a public body. Protection should also be afforded to those who release information disclosing a serious threat to health, safety or the environment, whether linked to individual wrongdoing or not. The absence of such protection in this Law is particularly a matter of concern, given that the FOI Law also lacks such protection.

Recommendation:

- The Law should provide protection to whistleblowers, unless such protection is written into the FOI Law.

III.9 Lack of Sanction for Wilful Misclassification

The Law fails to provide for a sanction for those who wilfully misclassify documents. In particular, the Law does not provide for sanctions for those who intentionally classify information for purposes of breach of the law, corruption or to limit the public's access to information.

Recommendation:

- The Law should provide for sanctions where information is wilfully misclassified.