TRANSPARENCY INTERNATIONAL
Defence and Security Programme

CORRUPTION RISKS

CORRUPTION RISKS SERIES

Classified Information

A review of current legislation across 15 countries & the EU

Preface

Transparency International UK's Defence and Security Programme works with governments, defence companies, and civil society organisations to reduce the risk of corruption in defence and security. Our approach is non-partisan, neutral and focused on constructive ways of addressing the issue of corruption.

This report, by Ádám Földes, former executive director of Transparency International Hungary and currently advocacy advisor in the Conventions Unit of Transparency International Secretariat, deals with the issue of freedom of information and its link to national security considerations.

The purpose of this report is to underpin that right to information provides the legal basis of transparency, which in turn is a precondition to establishing a system of real accountability. There is no reason why a functional defence and security sector cannot coexist with legal codes which allow for access to information, transparency and accountability.

By reviewing the freedom of information and security classification legislation of sixteen regimes, it is argued that national security and defence considerations can and should no longer be concealed from the majority of the population.

Accordingly, civil society requires more insight and better guarantees concerning security measures that are relevant to them.

We hope that this report will inform the public debate about what are the appropriate ways to balance national security information and the public's right to information.

Programme Director
Defence and Security Programme
Transparency International UK
February 2014

Contents

Executive summary

This report reviews the security classification legislation of fifteen countries which have grappled with the need to balance national security concerns with granting citizens the right to access information.

www.defenceindex.org
www.ti-defence.org

New anti-terrorism and national security legislations have for the most part reduced transparency and accountability.[1] All of the countries analysed in this study have grappled with the need to balance national security concerns with granting citizens the right to access information both in terms of legislations and legal jurisprudence. This report reviews the security classification legislation of fifteen countries and one supranational organisation: Austria, Australia, Czech Republic, Germany, Estonia, Hungary, Lithuania, Macedonia (FYR), Mexico, New Zealand, Poland, Republic of South Africa, Slovenia, Sweden, United Kingdom and the European Union. The report has also analysed the system in the United States, though not at the same level of depth. A short discussion of NATO information standards is also covered as an annex. The purpose is to provide a solid base of knowledge of what constitutes good and bad practice.

Parallel with the change in national security policies, freedom of information (FOI) has been gradually gaining ground all over the world. This development is definitely positive for raising the accountability and transparency of defence and security forces. Traditionally inaccessible national security and defence sectors increasingly have to accommodate new values of transparency and accountability. For instance, to raise the transparency of defence budgeting while mitigating the risk of exposing highly sensitive security-related information, the South Korean government separates the defence budget into three categories, depending on the degree of secrecy. Category 'A' budget items are presented for discussion to the entire National Assembly in an aggregated form; Category 'B' budget items are revealed to members of a designated National Assembly Committee of National Defence in a disaggregated and detailed form; and Category 'C' items are further disaggregated and presented only to the Committee of National Defence.[2]

Good practice in secrecy classification legislation includes rules on the following:

1. any restriction on right to information has to meet international legal standards which have to be also present in the applicable national legislation;

2. the authority to withhold or classify information needs to be well defined and has to originate from a legitimate source of power and be performed in line with procedures prescribed by published legal rules;

3. information may be protected by classification and/or exempted from disclosure if there is a real and substantial likelihood that its disclosure could cause serious harm;

4. if information is withheld there should be procedures (accessible to all) that allow for substantial review by independent bodies.

By highlighting the different legal mechanisms that exist in the sixteen regimes studied, governments, practitioners, and analysts can identify what constitutes good and bad practice in this sphere. For instance Mexico, the only Latin American country in the study, exhibits good practice in access to information by oversight bodies, time limits for period of classification, procedures to follow when declassifying information, external review of classification procedure, and prohibited classifications. Similarly, the United States, despite not being a core country of study for this report, highlights good practice examples in the scope of freedom of information laws, automatic declassification procedures, prohibited classifications & information of public interest, and time limits for period of classification. Further, New Zealand also highlights good practices in access to information by oversight bodies, declassifications, access to national security information, and protective markings.

On the other hand, the report also features the negative practices that some countries adopt. The Polish law, for instance, allows for eternal classification of certain sensitive data. To similar effect in Lithuania the classification period of state secrets can be extended by 10 years as many times as needed.

Of the countries examined in this study, Austria is perhaps the farthest behind global trends as it has failed to accommodate either the developments of the right of access to information or to introduce transparency measures into its classification system. The Austrian system is an anomaly in Europe since secrecy is still the default position and access to information is treated as an exception.

Further, little is known about the information standards within NATO since not many documents on the subject are made public. However, from the few that are, a number of weaknesses in the system are highlighted. These include not defining rules of protection and thus making the system prone to arbitrary classifications, not listing the subjects which may require classification, and not developing an expiry of classification periods.

Rules on secrecy classification legislation need to be supported by additional safeguards, notably the following:

1. Guarantees that no information be withheld from the public for an indefinite period;

2. Classifications and decisions on withholding information have to be justified in writing and information has to be properly archived for present and historical purposes;

3. The law should provide for a public interest test of weighing public interest in withholding and disclosing information or even prohibiting non-disclosure of certain categories of information;

4. There should be a maximum expiry time in every secrecy regime;

5. Active engagement of civil society in this sphere.

From this study it is clear that only a few countries contain these key safeguards in law.

As an overarching element to the above, the active engagement of civil society in this sphere is critical. Since there is an evident tension between the rules of freedom of information and of classification, civil society organisations need to provide crucial monitoring and oversight in both ensuring that the state does not indiscriminately classify information which is not sensitive to national security, and that citizens have access to information they have the right to see.

Introduction

The last few years have seen a major shift in the national security policies of countries that have the highest military expenditures.[3] France, Russia, the United Kingdom and the United States have adopted new national security strategies; in Germany the governing parties have prepared a draft security strategy, but as of December 2012 it had not been adopted.[4] None of these states perceive conventional threats by other countries, and the emphasis in these documents has shifted from classical sovereignty and territorial integrity issues to risks of international terrorism, nuclear proliferation, economic stability, organised crime, cyber-attacks, climate change and natural hazards, crisis management and protection of critical infrastructure. The safety and security of citizens have become the top priority – listed before the classical national security values.[5] Though it may be too early to declare that there is a clear universal tendency to replace the classical approach with this new outlook, signs of it are already visible in the written and published national strategies of arguably some of the world's most powerful countries.[6]

Along with this new approach, commitments to the principles of transparency and accountability have appeared in these strategies. Whilst Parliamentary and budgetary accountability of armed forces has been present since the inception of the parliamentary system, current policies show a significant change in this area. For instance, as a matter of strategic context the Government of the UK holds that 'our actions will be subject to scrutiny in the media and courts and by society at large'.[7] At the same time, in the chapter on British values, it is declared that 'National security is about protecting our people – including their rights and liberties – as well as protecting our democratic institutions and traditions. (...) To protect the security and freedom of many, the state sometimes has to encroach on the liberties of a few: those who threaten us. We must strike the right balance in doing this, acting proportionately, with due process and with appropriate democratic oversight'.[8] The French White Paper on defence and national security was prepared in an open manner which included 'far-ranging publicly televised and on-line hearings of some 52 personalities, from 14 countries and 5 continents' as well as involvement of think-tanks, academia and the broader public through online forums.[9]

The change in national security policies is coupled with the remarkable development of freedom of information laws. Currently more than ninety countries recognise the right of access to information, whereas only a fragment of them had such laws before the end of the Cold War. Right to information provides the legal basis of transparency which is a prerequisite to establishing any system of accountability. As the wider set of entities (e.g. courts, parliamentary commissioners/ombudspersons, NGOs, media) and the public at large gain roles in setting national security and defence policies, and in exercising scrutiny over defence and national security activities and spending, more refined legal regulation is needed to provide them with access and at the same time to ensure the security of information, personnel, installations, and assets.

The emergence of freedom of information laws is also being accompanied by reforms of classification regimes. Such developments affect not only the new democracies of Central and Eastern Europe and of Latin America, but also the secrecy regimes of several Western democracies. They have also received a facelift or total recast during the last two decades, even if some of them – i.e. Spain[10] or France[11] – fell short of performing this reform so far. In the last three or four years a rather diverse set

of countries have adopted or are going to adopt new secrecy rules (some of them along with new freedom of information rules), such as Australia,[12] Brazil,[13] China,[14] Estonia, Hungary,[15] Indonesia,[16] Poland, Republic of South Africa,[17] Serbia,[18] Sweden and Ukraine.[19]

The new freedom of information laws across the world are likely to also attract reforms of the secrecy regimes in many more countries. Such changes are also fostered by bilateral agreements in a wide range of topics such as on countering international terrorism, nuclear proliferation, organised crime, and cyber-attacks, where it is a practical element of the agreement to ensure the compatibility of various classification systems that enable exchange of information. It is also a prerequisite of the accession of countries to international organisations such as the NATO or the European Union to comply with their standards.

Transparency International has campaigned for over ten years on the need for greater access to information in the struggle against corruption. In 2003, it devoted a Global Corruption Report to the issue and highlighted how civil society, the public and private sectors and the media use and control information to combat or conceal corruption.[20] It is a subject of great importance for the organisation and one that has gained added significance due to recent calls around the world for more open and inclusive governments.

Transparency International UK's Defence and Security Programme works with governments, defence companies, multilateral organisations and civil society to build integrity and reduce corruption in defence establishments. Due to the secretive nature of the industry and the fact that many decisions are hidden from public view by the guise of national security considerations, the issue of freedom of information is very relevant to the programme.

By publishing this document, Transparency International UK aims to aid policy and decision-makers, civil society organisations, researchers and the media in finding the good practices that ensure at the same time confidentiality, integrity and availability of national security and defence information and the fulfilment of the principles of transparency and accountability in the defence and security sector.

The information in this report is correct as of August 2013.

ACKNOWLEDGEMENTS

We would like to thank the Open Society Justice Initiative and Access Info Europe. The joint work with the Defence and Security Programme of Transparency International was supported by a grant from Trust for Civil Society in Central and Eastern Europe within the framework of the Individual Development Grants Program of the School for Leaders Association. We would also like to thank the very useful legal analysis of Meredith Fuchs (The National Security Archive) on the US classification system, the pragmatic insights of Sir Stewart Eldon on national security policies, the useful comments on Lithuania by Rüta Mrazauskaité and on Germany by Christian Humborg. This study would have never been finished without the review by David Banisar, based on his vast expertise in this field – a special thanks to him.

Glossary

A: Austria
Informationssicherheitsgesetz, InfoSiG [Security of Information Act][21]

AFOI: Austria
Auskunftspflichtgesetz [Duty to Grant Information Act][22]

Ar: Austria
Informationssicherheitsverordnung, InfoSiV [Security of Information Regulation Act][23]

AU2007: Australia
Freedom of Information Guidelines – Exemption Sections in the FOI Act, Prepared for the Department of the Prime Minister and Cabinet as at 31 December 2007

AUFOI: Australia
Freedom of Information Act 1982

AUINFOSEC: Australia
Information security management guidelines – Australian Government security classification system, (version 1.0)[24]

CZ: Czech Republic
Act N. 412 of 21 September 2005 on the Protection of Classified Information

CZFOI: Czech Republic
106/1999 Coll. Act of 11 May 1999 on Free Access to Information

CZr: Czech Republic
Government Regulation N. 522 of 7 December 2005 Establishing the List of Classified Information[25]

D: Germany
VS-Anweisung - VSA vom 31. März 2006 mit Erläuterungen [General Administrative Instructions for the physical and organisational protection of classified material (Classified Material Instructions) issued by the Federal Ministry of the Interior on 31 March 2006][26]

DFOI: Germany
Informationsfreiheitsgesetz – IFG (Freedom of Information Act)

new EST: Estonia
State Secrets And Classified Information Of Foreign States Act -passed on 25 January 2007[27]

old EST: Estonia
State Secrets Act - passed on 26 January 1999[28]

ESTFOI: Estonia
Public Information Act[29]

EU: European Union
Council Decision of 31 March 2011 on the security rules for protecting EU classified information (2011/292/EU)

EUFOI: European Union
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

FOI: Freedom of Information

old HU: Hungary
Act LXV of 1995 on State and Service Secrets

new HU: Hungary
Act CLV of 2009 on Protection of Classified Information

HUFOI: Hungary
Act CXII of 2011 on Informational Self-Determination and Freedom of Information

LIT: Lithuania
Law on State Secrets and Service Secrets - November 25, 1999. No. VIII - 1443[30]

LITFOI: Lithuania
Law on provision of Information to the Public

MK: Macedonia (FYR)
Law on Classified Information[31]

MKFOI: Macedonia (FYR)
Law on Free Access to Information of Public Character[32]

MX: Mexico
Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental[33]

MXr: Mexico
Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

NZ: New Zealand
Security in the Government Sector – Department of the Prime Minister and the Cabinet 2002[34]

NZFOI: New Zealand
Official Information Act 1982[35]

old PL: Poland
The Classified Information Protection Act of 22 January 1999[36]

PLFOI: Poland
Law on Access to Public Information

RSA: Republic of South Africa
Minimum Security Information Standards[37]

RSAFOI: Republic of South Africa
Promotion of Access to Information Act[38]

SL: Slovenia
Classified Information Act[39]

SLFOI: Slovenia
Access to Public Information Act

SW: Sweden
Public Access to Information and Secrecy with Swedish Authorities (revised edition 2009)[40]

SWFOI: Sweden
The Freedom of the Press Act

UK2009: United Kingdom
HMG Security Policy Framework, v 2.0, May 09

UK2012: United Kingdom HMG Security Policy Framework, Version 8, April 2012[41]

UKFOI: United Kingdom
Freedom of Information Act 2000

US EO: United States
Executive Order 13526 - Classified National Security Information[42]

US FOIA: United States
The Freedom of Information Act 5 U.S.C. § 552

1. Nature of the study

This study has a rather specific scope. It looks at the detailed legislation on freedom of information and secrecy classification in a wide range of countries. We look for good legislative solutions that satisfied both the requirements of protecting national security and defence information and provide sufficient transparency to ensure accountability of this sector.

We have examined the freedom of information legislations, concerning national security and defence information, and the classification rules of sixteen legal systems: Austria, Australia, Czech Republic, Germany, Estonia, Hungary, Lithuania, Macedonia (FYR), Mexico, New Zealand, Poland, Republic of South Africa, Slovenia, Sweden, United Kingdom and the European Union. Further, the report has analysed the legal system in the United States, though not at the same level of depth. For this reason, when the report makes reference to 'all countries' in its analysis, it is important to note that this refers to the 15 countries and the EU, and *not* the United States or any other legal system which may be mentioned from time to time. We do not purport to be experts of all these legislations, nor do we suggest that these were the entirety of legal systems to assess. These countries were chosen on the basis that their legislation, either through the original legal texts or by translations, were easily accessible and available online. Constitutional provisions, freedom of information acts, secrecy acts and other lower level norms of continental and common law systems, new and old democracies, different traditions of public administrations, and countries of different importance in international politics were analysed. Most of the examined countries had authoritarian or dictatorial periods in their past which is occasionally reflected in their legal rules. Ten out of the fifteen countries are members of the European Union, eight are NATO members and a further three are NATO partners. A short discussion of NATO information standards is provided in Annex I.

In our analysis we focused on identifying common structures and patterns of various legislations. We found that legal structures in this field are comparable and not only amongst those that share a common legal tradition. Although eventually we refer to these traditions, we don't enter into historical particulars in this paper. Our aim is to identify good practices applied to identical legal situations so as to help policy makers and legislators when reviewing and modernising rules on protection of national security and defence information. The examples provided serve as illustrations of good solutions to various legal problems that arise in this complex field. In none of the chapters did we aim to describe all legal solutions of the sixteen regimes, therefore some legal systems may be under or over represented. The study has limited examples from the United States due to the availability of information and analysis on the subject. We relied on it where it was essential either as it is the best piece of regulation concerning a legal solution or where its provisions were used as a master plan by other countries in their respective regulations.

We are also aware of the axiom that legal provisions cannot be extracted from their context as they function in accordance with further provisions of the law. However, we believe that many of the represented examples can function in most of the freedom of information and classification regimes if transposed carefully.

The description of legal structures and good provisions are underpinned by the Tshwane Principles – Principles on National Security and the Right to Information (hereinafter referred as **Principle(s)**) that provide guidance to legislators and legal practitioners.[43] The present study can be used in three ways: First, as a stand-alone document that elaborates on all problematic areas of harmonising the concurring right of access to information and public interest in protecting national security and defence information. Second, it can be read as a commentary on the Principles (see below), though it does not address basic notions of freedom of information and neither extends its limits over the fields of freedom of information, protection of classified information and their relation to national security, while the Principles cover a wider range of issues. Third, the report could be read as a manual for both legislatures and advocates to write new freedom of information laws by looking at the good practice examples elucidated in this report. The findings in this report are based on research conducted until December 2012. Best effort has been made to ensure that all major changes in legal provisions up to that date have been reflected in the report.

2. Principles on national security and the Right to Information and their origin

In 1995, not long after the democratic transition in the Republic of South Africa 'a group of experts in international law, national security, and human rights convened by ARTICLE 19, the International Centre Against Censorship, in collaboration with the Centre for Applied Legal Studies of the University of the Witwatersrand, in Johannesburg' drew up a set of 'Principles on National Security, Freedom of Expression and Access to Information'.[44] The aim was to discern principles of international and regional law and standards. Further, practices of states and their courts in addressing conformity to freedom of expression and access to information with regards to the public interest is also addressed. The Principles 'have been endorsed by Mr. Abid Hussain, the UN Special Rapporteur on Freedom of Opinion and Expression, in his reports to the 1996, 1998, 1999 and 2001 sessions of the United Nations Commission on Human Rights, and referred to by the Commission in their annual resolutions on freedom of expression every year' between 1996 and 2003.[45]

The international legal standards and the interpretations of national security have changed significantly since 1995. In 2011, a new series of meetings started with the aim of preparing new principles on the basis of the Johannesburg Principles 'in order to provide guidance to people engaged in drafting, revising or implementing laws or provisions relating to the government's authority to withhold information on national security grounds or to penalize the publication of such information'.[46]

The Tshwane Principles (named after the place of the final meeting in South Africa) were published 12 June 2013 and included more than 500 experts from more than 70 countries who met at 14 meetings. In the drafting procedure the four special mandates on freedom of expression were also consulted: the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organisation for Security and Cooperation in Europe (OSCE) Representative on Freedom of the Media, the Organisation of American States (OAS) Special Rapporteur on Freedom of Expression, and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information.

The Principles on National Security and the Right to Information cover more than the title suggests. Principles on the relationship between national security and freedom of expression, whistle-blower's protection, oversight bodies, and judicial oversight are also set out.

3. Overview of the national security information and classification regimes and relevant requirements of international law

In this chapter, the outlines of the protection of classified information are explained. How classification regimes integrate with freedom of information rules, what are the underlying formal mechanisms and what is the substance of the classification of information.

Freedom of information is widely recognised by international law in numerous international conventions, such as the Universal Declaration of Human Rights (Article 19), International Covenant on Civil and Political Rights (Article 19), African [Banjul] Charter on Human and Peoples' Rights (Article 9); American Convention on Human Rights (Article 13) and the European Convention on Human Rights (Article 10). At the same time international law also recognises that limitations of this right may be necessary for the protection of national security. Both the exercise of the right and its limitations are detailed in national legislations which are regularly interpreted by national and international courts (e.g. by the European Court of Human Rights, by the Inter-American Court of Human Rights) as well as by other international bodies.

As the International Covenant on Civil and Political Rights (ICCPR)[47] has 167 Parties, it is worth briefly examining how Article 19 of it provides for both freedom of expression and freedom of information. 'Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice'.

The same article regulates the possible restrictions on these rights: '[t]he exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals'.

The Human Rights Committee (established by the ICCPR) interpreted this provision as 'when a State party imposes restrictions on the exercise of freedom of expression, these may not put in jeopardy the right itself. The Committee recalls that the relation between right and restriction and between norm and exception must not be reversed. […] Restrictions are not allowed on grounds not specified in paragraph 3, even if such grounds would justify restrictions to other rights protected in the Covenant. Restrictions must be applied only for those purposes for which they were prescribed and must be directly related to the specific need on which they are predicated'.[48] Furthermore in its practice on Article 19 paragraph 3b, to satisfy the Committee '[t]hat a particular restriction on freedom of expression is necessary, a State must make a three-part showing. The State must establish that: (1) there exists a threat to the nation as a whole; (2) the expression at issue has caused or contributed to that threat; and (3) the restrictive measures are necessary to prevent the threat and proportional to it'.[49]

Before the U.N. Human Rights Council another three-part test was presented regarding the application of the above mentioned optional restrictions under Article 19: '(a) the restriction must be provided for by law; (b) it must pursue a legitimate aim; and (c) it must be necessary and proportionate to secure one of those aims'.[50] The same author interpreted Article 19 of ICCPR in light of the practice of the European Court of Human Rights (hereinafter: ECtHR).[51] [F]or a restriction to be legitimate, all three parts of the test must be met:

1. 'First, the interference must be provided for by law. This requirement will be fulfilled only where the law is accessible and "formulated with sufficient precision to enable the citizen to regulate his conduct".[52]

2. Second, the interference must pursue a legitimate aim. The list of aims in the various international treaties is exclusive in the sense that no other aims are considered to be legitimate as grounds for restricting freedom of expression.

3. Third, the restriction must be necessary to secure one of those aims. The word "necessary" means that there must be a "pressing social need" for the restriction. The reasons given by the State to justify the restriction must be "relevant and sufficient" and the restriction must be proportionate to the aim pursued.'[53]

There is another test for the 'narrow interpretation' which in practice would mean that a law restricting the rights of freedom of expression and freedom of information carries more weight if it serves directly the exercise and protection of another fundamental right (e.g. right to privacy), less if it protects such rights indirectly through some intermediary institutions, and the least if it concerns some abstract values such as public order.[54] In regards to protection of classified information – in most cases – the restriction of the right of access to information serves the protection of abstract values i.e. various public interests. The more distant the public interest to the restriction of the right of access to information, the higher the risk of unconstitutionality or the risk of the breach of international norms will be, and the less likely the legal provisions will be complied with.

Principle 1 of the Principles on National Security and the Right to Information summarises the right and limitations, based on international norms and in favour of robust transparency, the following way:

a. 'Everyone has the right to seek, receive, use, and impart information held by or on behalf of public authorities, or to which public authorities are entitled by law to have access.

b. International principles also recognize that business enterprises within the national security sector, including private military and security companies, have the responsibility to disclose information in respect of situations, activities, or conduct that may reasonably be expected to have an impact on the enjoyment of human rights.

c. Those with an obligation to disclose information, consistent with Principles 1(a) and 1(b), must make information available on request, subject only to limited exceptions prescribed by law and necessary to prevent specific, identifiable harm to legitimate interests, including national security.

d. Only public authorities whose specific responsibilities include protecting national security may assert national security as a ground for withholding information.

e. (e) Any assertion by a business enterprise of national security to justify withholding information must be explicitly authorized or confirmed by a public authority tasked with protecting national security.

Note: The government, and only the government, bears ultimate responsibility for national security, and thus only the government may assert that information must not be released if it would harm national security.

f. Public authorities also have an affirmative obligation to publish proactively certain information of public interest.'

If we look at the national legal regulations of the sixteen examined countries, we find that the most refined and best publicly documented freedom of information and classification system functions are in the USA. It is partially due to the fact that its freedom of information law has a history of almost half a century, which may seem very short compared to history of criminal or civil law, but rather significant in a field where only two countries took precedent before its adoption in 1966.[55] It could also partially be explained by the very strong traditions of the freedom of speech and freedom of the press which always facilitate the development of freedom of information. The most integrated freedom of information and classification system may be the Mexican example as established by the Federal Transparency and Access to Governmental Public Information Act. This is a rather progressive legal instrument as it regulates the two areas in the same piece of legislation.[56]

The Austrian legislation is possibly the one which is the farthest behind the global trends and failed to accommodate either the developments of the right of access to information or to bring any transparency to their classification system. The Austrian system is a curiosity in Europe as it states that not only is some information protected in the interest of the public/country/nation, but it is enshrined in the Federal Constitution that secrecy is still the default rule and access to information is an exception. This provision has the same origins as the Anglo-Saxon official secrets acts, however during the last decades those countries with official secrets acts adopted and implemented functional freedom of information laws, unlike Austria.

3.1 MODELS OF REGULATING FREEDOM OF INFORMATION AND CLASSIFICATION OF INFORMATION

As stated previously, everybody has the right to seek information. On a practical level this means that anyone can send a letter, an e-mail or request in person to access information or documents. Legislations may vary whether the ‘anyone’ has to be a citizen of that country or not. The definition of information and document, as well as the means of requesting, can also be regulated in various ways. Yet regardless of these details, it is common in all legal systems that the requested authorities have to deal with the incoming requests by following their applicable laws. If the requestor refers to legal norms to emphasise his/her right to know, or the requested official is for any reason looking for (legal) arguments why the requested piece of information cannot be disclosed, then legal machinery comes to the fore. This is especially true for information concerning national security or defence which always call for the special attention of the requested public officials.

‘Secrecy thus expresses two different aspects of the same matter: if the public is not entitled to obtain an official document, the authorities and the public officials are consequently forbidden from making the document available or disclosing its contents in another way. […] Furthermore, secrecy also means that information may not be made available to *other Swedish authorities* in cases other than those stated in the Public Access to Information and Secrecy Act or in an enactment or an ordinance to which the Public Access to Information and Secrecy Act refers. To a certain extent, secrecy also applies *within an authority*, namely between various operational branches within an authority where these are to be considered to be independent in relation to each other. Finally, secrecy means that information may not be disclosed to *foreign authorities or international organisations* except if the disclosure is made in accordance with a special rule contained in an Act or Ordinance or under certain preconditions specified in the Public Access to Information and Secrecy Act. […] If secrecy applies to information, then nor may the information be exploited outside the operation where it is subject to secrecy (for example, for stock-exchange speculation)’. (SW 3.3, 3.5.2, 3.5.1).

"Public Access to Information and Secrecy with Swedish Authorities (revised edition 2009)"

When somebody requests access to or disclosure of information on national security or defence the request triggers **two parallel mechanisms**. The first one is the application of the freedom of information law of the country, if available. The second is the application of rules on protection of classified information or state secrets. The basic meaning of freedom of information has been described above, and its details are defined by the laws of approximately 90 countries around the globe and by numerous international legal instruments.[57]
In the international legal framework, as well as in national legal systems, the right of access to information has been gradually gaining the status of a human right. The latest General Comment of the UN Human Rights Committee interpreted Article 19, paragraph 2 of the ICCPR that ‘embraces a right of access to information held by public bodies’.[58]

The parallel system of protection of classified information has a different objective: the disclosure of unauthorised access to certain information (e.g. national security, defence, foreign relations) may pose an above-average threat to public or private interests, therefore heightened level of protection should be provided. The procedure of determining the adequate level of protection needed for the piece of information is the classification.

Without considering the rules of international law, generally these parallel systems are regulated at least on two levels in any national legal system, if at all. The **first level** is the constitution where usually restriction of freedom of information is allowed in very general terms and it refers to other laws for further details. However, some constitutional laws are explicit on national security restrictions. In the Czech Republic ‘the freedom of expression and the right to information are guaranteed. (...) The freedom of expression and the right to seek and disseminate information may be limited by law in the case of measures that are necessary in a democratic society for protecting the rights and freedoms of others, the security of the state, public security, public health, or morals’.[59] In Poland, limitations ‘may be imposed by statute solely to protect freedoms and rights of other persons and economic subjects, public order, security or important economic interests of the State’.[60]

The **second level** is set by act(s) of the Parliament where two main models of protection can be identified. Although the models differ in many aspects, some common features of these systems can be captured.

In the ***single act model,*** information which needs a higher level of protection is exempted under the FOI Act. Further, there are policies, manuals, regulations, and directives on its protection. These rules are binding only on those public bodies, public officials or other persons who are authorised to hold, handle, access or use such information. Other individuals are not bound by these rules (Australia, European Union, New Zealand, Germany, Republic of South Africa, United Kingdom, United States).[61]

In the ***double act model,*** information which needs a higher level of protection is exempted under the FOI Act and usually a separate act of the Parliament regulates their protection which is binding on all (Austria, Czech Republic, Estonia, Hungary, Lithuania, Macedonia (FYR), Mexico[62], Poland, Slovenia, Sweden).

There is also a third type, a ***non-model,*** where either there are no clear rules on what is considered as information which needs a higher level of protection or rules exist but are not published. If the rules are unpublished, then those who are subject to the law cannot foresee the consequences of their actions, thus any sanction for violating these rules will inevitably be arbitrary and contrary to the fundamental principles of the rule of law.[63]

3.2 PUBLIC ACCESS TO CLASSIFICATION RULES

As detailed above, Article 19 of the International Covenant on Civil and Political Rights contains optional restrictions. The first element of a restriction is that it must be provided for by law. Any norm which is claimed to be law must be public and accessible by anyone to take any effect on citizens. Secrecy laws are no exception, though the first element of the three-part test 'prescribed by law' is highly problematic in this field.

General Comment No 34 of the UN Human Rights Committee spells out that the

> 'Law may include laws of parliamentary privilege and laws of contempt of court. Since any restriction on freedom of expression constitutes a serious curtailment of human rights, it is not compatible with the Covenant for a restriction to be enshrined in traditional, religious or other such customary law.
>
> For the purposes of paragraph 3, a norm, to be characterized as a "law", must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution. Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not.' *(references omitted)*[64]

The ECtHR also discussed this requirement, regarding Article 10 of the ECHR (freedom of expression), in the case of the Sunday Times v. United Kingdom.

> 'In the Court's opinion, the following are two of the requirements that flow from the expression "prescribed by law". Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail. Those consequences need not be foreseeable with absolute certainty: experience shows this to be unattainable. Again, whilst certainty is highly desirable, it may bring in its train excessive rigidity and the law must be able to keep pace with changing circumstances. Accordingly, many laws are inevitably couched in terms which, to a greater or lesser extent, are vague and whose interpretation and application are questions of practice'.[65]

The US Supreme Court found similar criteria on the clarity of laws.

> 'It is a basic principle of due process that an enactment is void for vagueness if its prohibitions are not clearly defined. Vague laws offend several important values. First, because we assume that man is free to steer between lawful and unlawful conduct, we insist that laws give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly. Vague laws may trap the innocent by not providing fair warning. Second, if arbitrary and discriminatory enforcement is to be prevented, laws must provide explicit standards for those who apply them. A vague law impermissibly delegates basic policy matters to policemen, judges, and juries for resolution on an *ad hoc* and subjective basis, with the attendant dangers of arbitrary and discriminatory application. Third, but related, where a vague statute "abut[s] upon sensitive areas of basic First Amendment freedoms," it "operates to inhibit the exercise of [those] freedoms." Uncertain meanings inevitably lead citizens to *"steer far wider of the unlawful zone' . . . than if the boundaries of the forbidden areas were clearly marked".*[66]

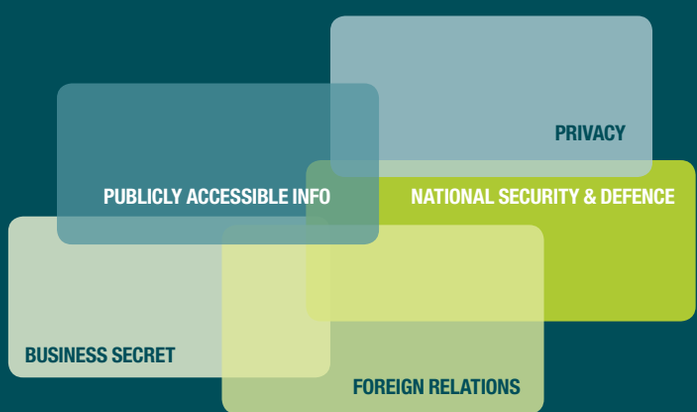
Even in well-established democracies details of regulations on classification of sensitive information might be inaccessible. In 2009, in the foreword of UK's HMG Security Policy Framework, the Cabinet Secretary admitted that '[f]or the first time the framework allows for much of this material to be placed in the public domain'.[67] In New Zealand, the Protective Security Manual, which is partially based on the predecessor of the HMG Security Policy Framework and complements the Security in the Government Sector Manual regarding the questions of classification (how much damage or prejudice would result from compromising specific content), has itself an overall classification of RESTRICTED.[68] In Australia, the Australian Government Protective Security Manual (PSM) was a government policy issued to all Australian Government agencies, but access to it was restricted to Government agencies. In 2011, the PSM was superseded by the Protective Security Policy Framework of the Australian Government of which Information security management guidelines are available to the public.[69] In India, the Manual of Departmental Security Instructions, which provides for the core provisions of classification procedure, is itself classified.[70]

Five years after the democratic transition in Hungary, the Constitutional Court abolished the entire classification system which was based on obscure legislation. Through an act of Parliament, certain information has been made fully available to the public for the first time.[71]

Principle 12 stipulates that 'the public should have access to the written procedures and standards governing classification' and 'the public should have the opportunity to comment on the procedures and standards governing classification prior to their becoming effective'.

It is a general requirement of open legislation – which is realised through different models depending on the country's political and legal culture – that both the scope of the laws on and the restrictions of the right of access to information should be publicly discussed, adopted and declared, in the same procedure as any other piece of legislation. In the countries of the *double act model* this requirement is fulfilled, as both laws on the freedom of information and the protection of classified information, are adopted by the Parliament – the procedure of which is public. Legislation on protection of classified information obviously restricts the freedom of information and consequently freedom of expression which 'is a necessary condition for the realization of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of human rights'.[72] Due to the far-reaching significance of these laws their adoption should involve the broadest spectrum of society, however in practice it seems not to be the case. In *single act model* countries, the public may influence only the scope and structure of exceptions of the freedom of information. Manuals, regulations, and directives will not have a direct application on them, and they can hardly find any opportunity to realise Principle 12. Obviously, those countries which belong to the *non-model* category utterly disregard this principle.[73]

FIGURE 1 : OVERLAPPING EXEMPTIONS



3.3 THE AIM OF RESTRICTING ACCESS TO INFORMATION

Beyond the requirement of any 'restriction must be provided for by law' there is a second element to the three-part test presented before the U.N. Human Rights Council: there should be a legitimate aim of restriction and in this case freedom of information may need to be restricted to protect an interest. These restrictions or exemptions may protect private interests (e.g. privacy, business secret) or public interests (e.g. national security, criminal investigations, defence, foreign relations). Most FOI regimes have subsystems tailored to a specific type of information. For example, commercial and other economic interests are protected through provisions on business secrets which may be regulated by civil codes or fair competition laws, while privacy is usually protected by personal data protection laws. The laws on access to information always use the presumption that information held by a public body or concerning public matters (such as exercising public authority or related to public funds) have to be accessible to anyone.

This is the main rule (lex generalis) and details may be regulated by more specialised legal provisions of the legal field concerned (lex specialis). In any well-functioning legal system the law on access to information defines which exemptions are legitimate in any piece of legislation and in the legal practice. If new exemptions are introduced and restrictions are not enshrined in the law on access to information, that may cause significant ambiguities in the application of laws.

It is a common feature of all FOI regimes that exemptions limit access in three dimensions: according to **topics, requestors** (Chapter 5) and **time** (Chapter 12).

Limitation according to **topics** is designed in the following way: International instruments providing for freedom of expression and information recognise certain public and private interests for the protection of which restrictions are allowed (see Annex II.).

The understanding of the national security based restrictions may seem rather simple at first glance, but in fact every single term of these provisions have been continuously interpreted and reinterpreted by several international courts and other fora. Furthermore, the explicit and the implicit content of these provisions are also subject to various interpretations.[74] National FOI laws establish exemptions which generally stay within the range set out by the international instruments when defining possible restrictions. These widely accepted grounds for exemptions include protection of the public interest[75], national interest[76], vital interest[77],permanent interest[78], interest of importance[79], state interest[80], essential interest[81], and fundamental interest[82]. These broad terms are further broken down to more specific topics. There might be a dozen of them, which cover, besides classical national security, foreign policy, and defence triplet, prevention or prosecution of crime, central financial policy / monetary policy, effective administration of justice, etc. and any of these exemptions may provide ground for classifying information as state secret. However, some legislations narrow down the definitions of state secrets: information 'which requires protection from disclosure in the interests of the national security or foreign relations of the Republic of Estonia with the exception of classified information of foreign states'.[83] In this case the term 'national security' still embraces the other topics as all of them may be elements of sovereignty and territorial integrity. In those cases when there is a pressing social need to provide them protection they can be withheld.[84] At the same time if a law stipulates that exclusively information concerning 'interests of the national security or foreign relations' can be protected as state secret it can be also understood as no information covered by other exemptions can be classified and protected as state secrets.

The Australian legislation sorts the exemptions into two classes: 'exempt documents (such as documents affecting national security, defence or international relations, Cabinet documents or documents affecting law enforcement and protection of public safety)' and 'conditionally exempt documents, where access is conditional upon meeting a public interest test (such as documents affecting Commonwealth-State relations or documents that are used for deliberative processes)'.[85] Documents belonging to the first class are not required to be disclosed but the decision-maker has the discretionary power to provide access, while in case of conditional exemption documents have to be disclosed as a main rule 'unless disclosure would be contrary to the public interest at the time of decision' (see details in Chapter 4.2).[86]

The third element of the three-part test is that the restriction should be necessary and proportionate. In secrecy regimes, the harm test and the public interest test are to ensure that the restriction is applied only when it is necessary (detailed in Chapter 2) and the proportionality of the restriction is achieved by the classification to different levels of protection (detailed in Chapter 5).

4. Criteria for providing protection to information by classification

The present chapter intends to reconcile the two very different approaches of 'need to know' (the originators of classified information) and of the 'right to know' (the public). Both withholding and disclosing information may serve the public interest, therefore very careful considerations and refined legal machinery have to support these goals.

There are several criteria that must be met if restrictions are to be imposed on the right of access to information on national security grounds. **Principle 3** on Requirements for Restricting the Right to Information on National Security Grounds has the following provisions:

'No restriction on the right to information on national security grounds may be imposed unless the government can demonstrate that: (1) the restriction (a) is prescribed by law and (b) is necessary in a democratic society (c) to protect a legitimate national security interest; and (2) the law provides for adequate safeguards against abuse, including prompt, full, accessible, and effective scrutiny of the validity of the restriction by an independent oversight authority and full review by the courts.

a. *Prescribed by law.* The law must be accessible, unambiguous, drawn narrowly and with precision so as to enable individuals to understand what information may be withheld, what should be disclosed, and what actions concerning the information are subject to sanction.

b. *Necessary in a democratic society.*

i. Disclosure of the information must pose a real and identifiable risk of significant harm to a legitimate national security interest.

ii. The risk of harm from disclosure must outweigh the overall public interest in disclosure.

iii. The restriction must comply with the principle of proportionality and must be the least restrictive means available to protect against the harm.

iv. The restriction must not impair the very essence of the right to information.

c. *Protection of a legitimate national security interest.* The narrow categories of information that may be withheld on national security grounds should be set forth clearly in law.

Notes: See definition of "legitimate national security interest"in the Definitions section, above. Principle 3(b) is all the more important if national security is not defined clearly in law as recommended in Principle 2.

"Public interest" is not defined in these Principles. A list of categories of especially high public interest that should be published proactively and should never be withheld is set forth in Principle 10. A list of categories of wrongdoing that are of high interest to the public, and that public servants should and may disclose without fear of retaliation, is set forth in Principle 37.

In balancing the risk of harm against the public interest in disclosure, account should be taken of the possibility of mitigating any harm from disclosure, including through means that require the reasonable expenditure of funds. Following is an illustrative list of factors to be considered in deciding whether the public interest in disclosure outweighs the risk of harm:

- *factors favoring disclosure: disclosure could reasonably be expected to (a) promote open discussion of public affairs, (b) enhance the government's accountability, (c) contribute to positive and informed debate on important issues or matters of serious interest, (d) promote effective oversight of expenditure of public funds, (e) reveal the reasons for a government decision, (f) contribute to protection of the environment, (g) reveal threats to public health or safety, or (h) reveal, or help establish accountability for, violations of human rights or international humanitarian law.*

- *factors favoring non-disclosure: disclosure would likely pose a real and identifiable risk of harm to a legitimate national security interest;*

- *factors that are irrelevant: disclosure could reasonably be expected to (a) cause embarrassment to, or a loss of confidence in, the government or an official, or (b) weaken a political party or ideology.*

  The fact that disclosure could cause harm to a country's economy would be relevant in determining whether information should be withheld on that ground, but not on national security grounds.'

There are two approaches to classification: a) the information is classified immediately, or b) it is classified when the public body holding the information receives a request and upon assessing the request considers the information as requiring protection under classification rules.

In the first case there are usually formal and substantive criteria to comply with, otherwise the classification will be invalid. The person classifying the information shall have **authorisation** to do so (Chapter 10) and the classification has to be performed in line with the **procedure** prescribed by law (Chapter 7). A **harm test** (see below) should be performed to assess the gravity of the harm and the probability of the harm that could result from unauthorised disclosure or loss of information concerning matters of interests protected by law (Chapter 3.3 and Chapter 4.3). The outcome of the harm test is the substantive basis of the classification. In some countries it is a further criterion that the information to be classified has to pertain to one of the **themes** in a list that forms part of the law (Chapter 4.3).

If the classification meets all the criteria, the information will be regarded as classified information which can be accessed, used, and disposed of according to higher standards of confidentiality, integrity and availability.

In the second case, the information gains its classified status only if there is an information request which triggers a harm test and possibly a public interest test, by an authorised person, in a procedure prescribed by law, and depending on the outcome of the test(s) information may be accessed, disclosed to the public or classified. There are also legal systems which allow for both approaches, for example that of Mexico.[87]

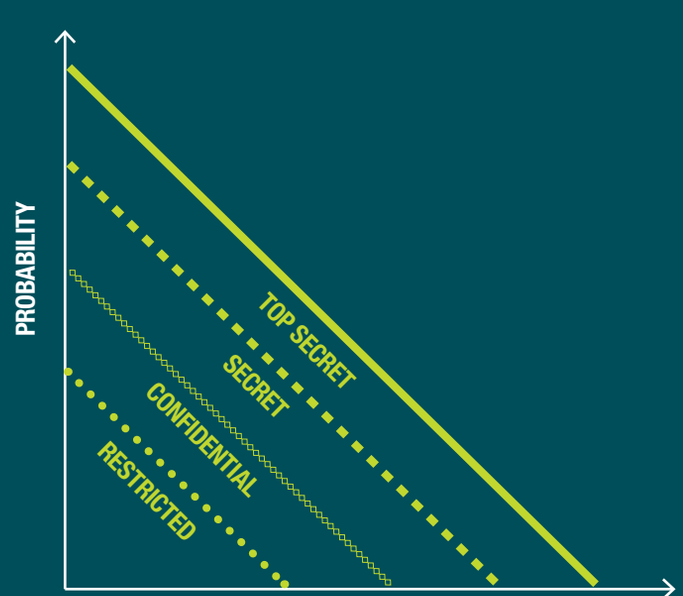
In Slovenia – which belongs to the first case – the initiation of the classification procedure precedes even the creation of the information as '[a]n authorised person shall determine the level of classification of information at the origin of that information, i.e. at the beginning of the performance of a task of the agency that results in classified information'.[88]

Another distinction to take into consideration is whether the law provides for the classification of *information* or of *entire documents (or even categories of documents and files)* or whether in some cases both are possible. This difference has practical relevance in cases of partial access when the same document contains both sensitive and classified information as well as information not protected as classified. The latter issue is usually regulated by general provisions of freedom of information laws and 'it is also well-established in practice that where only part of a record is confidential, the rest should still, if possible, be disclosed'.[89]

4.1 HARM TEST

Ideally a harm test is an assessment of possible harms which may be caused to a concrete public interest; however in practice, occasionally, public interests assessed in the test are not very concrete. In Chapter 3.3, typical protected interests found in different legal systems were discussed, which in fact tend to resemble

FIGURE 2: HARM ASSESSMENT



each other. The same interests are protected if we examine classification systems. There is however one significant difference between these legal provisions - namely whether the probability of threat or harm (damage)[90] is a requirement for the classification of information.

The rules defining the assessment usually have two components: the *gravity* of the harm and the *probability* of the harm. In every secrecy law the composition of these elements is different, however each one sets up a system in which, commensurate with the gravity and probability of harm, the higher level of protection shall be provided to the classified information.

Legislative approaches for the assessment of probability have a wide range. At one end there is a rigid scheme where the legislator determines probabilities of harm solely on the basis of the content of information (former Estonian law), while on the other end there is a flexible setting where public officials have to assess the possible harms on a case by case basis (e.g. Czech Republic).[91]

The former UK security policy prescribed that

> 'the originator or nominated owner of information, or an asset, is responsible for applying the correct protective marking. When protectively marking a document, it is recommended that a damage or 'harm test' is conducted to consider the likely impact if the asset were to be compromised and to help determine the correct level of marking required. 'The "harm test" should be done by assessing the asset against the criteria for each protective marking'.[92]

Similarly, in the Czech law '[i]n determining the level of classification, the authorised person shall assess the possible adverse effects of the disclosure of information to unauthorised persons on the security of the country or on its political or economic interests. On the basis of that assessment the authorised person shall determine the level of classification, after which the information shall receive the markings prescribed by this Act.'[93]

In the New Zealand guidelines the harm test is applied, albeit without using any modal verbs (that are usual in all other examined laws) to refer to probable, yet uncertain events.[94]

The unauthorised access or disclosure in the Czech Republic 'could cause damage to the interest of the Czech Republic or could be unfavourable to this interest'; in the Polish law 'exceptionally grave harm' to the state's legal interests[95] or 'expose those interests to no less than a substantial damage'[96]; in the Lithuanian law 'disclosure of which may present a threat to', 'may inflict damage',[97]; in the EU 'disclosure of which could cause varying degrees of prejudice'[98]; in the Hungarian law 'directly harms or threatens'[99]; in Australia 'would or could reasonably be expected to cause damage to'[100]; and according to the Macedonian provisions 'disclosure of which would put in jeopardy and cause irreparable damage'[101] to the public interests enlisted.[102] The definitions of state secrets / classified information in Austria, Germany, Mexico, Republic of South Africa and Slovenia also contain both gravity and probability of harm elements.

It is noteworthy that these harm tests in practice face significant challenges. As the Public Interest Declassification Board of the United States pointed out in its report 'estimating the level of damage that might result from unauthorised release is often an exercise in speculation and more art than science, particularly when prediction of damage is inconclusive'.

Agencies often make these decisions in isolation, without input from other classifying agencies or knowledge of prior declassification actions. The vagaries in this process lead to imprecise and excessive classification'.[103]

4.2 PUBLIC INTEREST TEST

Even if it is already established by a harm test that the disclosure would cause harm, it does not necessarily mean that the requested information should not be disclosed. There can be cases when the non-disclosure of sensitive information, held by public bodies, causes more harm than the disclosure, such as in cases of environmental disasters or food security hazards (Chapter 8).[104] When assessing the relationship of public interest and disclosure it is noteworthy that '[t]he public interest has been described as something that is of serious concern or benefit to the public, not merely of individual interest [reference omitted]. It has been held that public interest does not mean of interest to the public but in the interest of the public'.[105]

Unlike the harm test, the public interest test can only be performed on request of information, as prior to a request one of the scale pans would be empty when measuring public interest in withholding information against public interest in disclosing it. A legal assessment of two public interests can be performed when both public interests are articulated. However, in some legislations (Chapter 8) instead of the body holding the information, the legislator performs the public interest tests based on few pre-defined categories of information. In these cases, it is an irrefutable presumption that public interest in disclosure prevails over public interest in withholding information, if the requested piece of information pertains to these pre-defined categories.

In half of the examined information regimes there are public interest tests and if there is one, in all cases it is included in the FOI Act and not in the secrecy rules. Furthermore, even if the FOI law has a public interest test, it does not always apply to classified information.[106] Such is the case with the EU legislation regarding all classified information and in Slovenia regarding information classified at the two highest levels of secrecy.[107] The United Kingdom's Freedom of Information Act provides for public interest tests which are applicable to the majority of exemptions. Information does not have to be disclosed if in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information.[108] Defence, international relations, and national security information (unless the latter was directly or indirectly supplied by, or relates to intelligence or security bodies enlisted in the FOI Act) are subject to a qualified exemption (meaning they are subject to the public interest test).[109] With regards to the national security exemption 'there are likely to be strong public interest factors in favour of maintaining the exemption and not disclosing the information. The information should nevertheless be released unless these factors outweigh the public interest in disclosure'.[110]

In Swedish law, '[t]he freedom to communicate does not mean that public officials are *liable* to provide information to the mass media but only that they have an opportunity to do so, if they consider that the interest of public access to the authorities' operations weighs more heavy than the interest to be protected by the secrecy'.[111]

In the Republic of South Africa, the test is formulated in a rather similar way 'the public interest in the disclosure of the record clearly outweighs the harm contemplated in

the provision in question'. The Official Information Act of New Zealand is similar.[112]

In Australia:

> '[T]he phrase 'public interest' appears in a number of exemptions in the FOI Act. The concept of public interest is given different applications in various areas of decision making, depending on the legislative or administrative purposes involved. The 1979 Senate Committee on FOI described the concept in the FOI context as a convenient and useful concept for aggregating any number of interests that may bear upon a disputed question that is of general – as opposed to merely private – concern. When considering whether documents can or should be released, the concept of the public interest requires a decision maker to weigh the public interest factors for and against disclosure and to decide, on balance, whether disclosure is in the public interest. In order to comply with the principles in the FOI Act, documents should be released unless the balance lies strongly against disclosure.'[113]

In a subsequent guide to the Australian FOI Act, it is further detailed that 'in this process a decision maker needs to identify factors favouring disclosure and factors not favouring disclosure, and to determine the comparative importance to be given to these factors'. The factors in favour of disclosure are whether the access promotes the objectives of the FOI Act, informs debate on a matter of public importance, promotes effective oversight of public expenditure, and allows a person to access his or her own personal information.

The same interpretation also warns that none of the following factors should be taken into consideration when a public interest test is performed: embarrassment to the Government, risks that 'access to the document could result in any person misinterpreting or misunderstanding the document', if 'the author of the document was (or is) of high seniority in the agency to which the FOI request was made' and if 'access to the document could result in confusion or unnecessary debate'.[114]

On a more specific level, the Information Commissioner's Office of the UK provide detailed suggestions on factors that would weigh in favour of disclosure when performing a public interest test concerning defence information: a) Furthering the understanding of and participation in the public debate of issues of the day, b) Promoting accountability and transparency by public authorities for decisions taken by them, c) Promoting accountability and transparency in the spending of public money, d) Bringing to light information affecting public health and public safety.[115]

The Slovene FOI Act provides a limited scope for public interest tests: '[w]ithout prejudice to the provisions in the preceding paragraph, the access to the requested information is sustained, if public interest for disclosure prevails over public interest or interest of other persons not to disclose the requested information, except in the next cases', which include among others information classified at the two highest levels of secrecy, classified information of other country or international organisation.[116]

In Estonia there is a public interest test, however it is limited to a specific area of internal information.

> 'A holder of information shall disclose information concerning facts which arouse public interest and which are related to an offence or accident before the final clarification of the circumstances of the offence or accident to an extent which does not hinder the investigation or supervision or clarification of the reasons for the accident. The competent official who organises the investigation or supervision or who clarifies the

circumstances of the accident shall decide on the extent of disclosue of such information.' [117]It may be only a translation question of the Macedonian law, but it allows not only disclosure, but publishing based on public interest test. 'Information holders shall allow access to information should, in case such information is published, consequences to the interest being protected be smaller than the public interest to be maintained with the publishing of such information'.[118]

4.3 CONTENT OF INFORMATION THAT LEGITIMATELY MAY BE WITHHELD

As mentioned above, in some countries it is a further criterion beyond the harm test and a possible public interest test that the information to be classified has to pertain to one of the **themes** in a list that forms part of the law. Many of the post-communist countries had, or still have, such lists and thier goal is to avoid over-classification. If the legislator has concerns that public officials are not be properly orientated, then terms such as 'could cause damage to the interest of the' or 'pose danger to' could act as a further check point.

RECOMMENDATION

Freedom of information laws should contain public interest tests with regard to all exemptions that may be applied to classified information.

Secrecy regimes should contain harm tests.

Both harm tests and public interest tests should comply with international standards with regard to requirements of necessity and proportionality, as established by international human rights forums.

Designating harm test provisions, assessment on a case by case basis performed by public officials should be preferred, as this scheme provides for more flexible correction mechanisms against unnecessary classification.

New provisions to effect the *conclusive certificate* should not be introduced and the current ones should be removed.

The effects of the list are debated. If it functions well, the public official has less room for manoeuvre when classifying information, and in case the information does not pertain to any of the themes enlisted, it cannot be classified. If it is dysfunctional, the list of themes may motivate public officials to classify information for the sole reason that it is enlisted and may not perform a proper harm test. If the list of themes functions well, there is still a question from the perspective of 'access is the main rule, secrecy is the exception', and also from the perspective of efficient information management: in which system do the exemptions cover less information?

The first annex of the old Polish secrecy act enlisted almost a hundred themes organised in three categories: "top secret"; "secret" for reasons of national defence and security of the state and for reasons of public order; and "secret" for reasons of important national interests. The other category of classified information in the former Polish law, the public service secrets, did not have such a list according to their legal definition.[119]

The present Czech, and the former Hungarian laws, divide the lists of themes into categories according to scope of responsibilities of public bodies, such as defence, culture, industry and commerce, etc. The Czech list contains more than 230 themes and at each theme the range of possible classification is indicated.[120] In Hungary, the annex of the former Hungarian secrecy act had a list of more than 150 elements. These were highlighted and eventually published in the Official Gazette. Before publishing the list, the Parliamentary Commissioner for Personal Data Protection and Freedom of Information had to be

PRINCIPLE 9

(a) Public authorities may restrict the public's right of access to information on national security grounds, but only if such restrictions comply with all of the other provisions of these Principles, the information is held by a public authority, and the information falls within one of the following categories:

i. Information about on-going defense plans, operations, and capabilities for the length of time that the information is of operational utility.
Note: The phrase "for the length of time that the information is of operational utility" is meant to require disclosure of information once the information no longer reveals anything that could be used by enemies to understand the state's readiness, capacity, or plans.

ii. Information about the production, capabilities, or use of weapons systems and other military systems, including communications systems.
Note: Such information includes technological data and inventions, and information about production, capabilities, or use. Information about budget lines concerning weapons and other military systems should be made available to the public. See Principles 10C(3) & 10F. It is good practice for states to maintain and publish a control list of weapons, as encouraged by the Arms Trade Treaty as to conventional weapons. It is also good practice to publish information about weapons, equipment, and troop numbers.

iii. Information about specific measures to safeguard the territory of the state, critical infrastructure, or critical national institutions (institutions essentielles) against threats or use of force or sabotage, the effectiveness of which depend upon secrecy;
Note: "Critical infrastructure" refers to strategic resources, assets, and systems, whether physical or virtual, so vital to the state that destruction or incapacity of such resources, assets, or systems would have a debilitating impact on national security.

iv. Information pertaining to, or derived from, the operations, sources, and methods of intelligence services, insofar as they concern national security matters; and

v. Information concerning national security matters that was supplied by a foreign state or inter-governmental body with an express expectation of confidentiality; and other diplomatic communications insofar as they concern national security matters.
Note: It is good practice for such expectations to be recorded in writing.
Note: To the extent that particular information concerning terrorism, and counter-terrorism measures, is covered by one of the above categories, the public's right of access to such information may be subject to restrictions on national security grounds in accordance with this and other provisions of the Principles. At the same time, some information concerning terrorism or counterterrorism measures may be of particularly high public interest: see e.g., Principles 10A, 10B, and 10H(1).

(b) It is good practice for national law to set forth an exclusive list of categories of information that are at least as narrowly drawn as the above categories.
(c) A state may add a category of information to the above list of categories, but only if the category is specifically identified and narrowly defined and preservation of the information's secrecy is necessary to protect a legitimate national security interest that is set forth in law, as suggested in Principle 2(c). In proposing the category, the state should explain how disclosure of information in the category would harm national security.

EXAMPLES OF THEMES:

'The location, connections and connection points of the telecommunications network of the Security Police Board and the Government Department of Communications, and information concerning the configuration, capacity, frequencies and other parameters of the network and the equipment thereof. A medium containing such information shall be classified for fifteen years.' old EST Art 6 para 8

'Information and documents from the areas of the military infrastructure and mobilization of the Armed Forces of the Czech Republic.' CZr, The list of classified information – general part point 2.

'The system and manner of protecting the state borders, of monitoring cross-border traffic, anti-terrorist and anti-sabotage measures, likewise information on the operational potential for protecting the state borders.' old PL Annex No 1. II. 32.

consulted, though there was no consequence if his opinion was disregarded.[121] The number of categories and themes vary, for example the Lithuanian secrecy act enlists only 28 themes of state secrets and 29 of official secrets. The Estonian secrecy law enlists various themes under headings of various public interests that need protection such as 'State Secrets Related to Foreign Relations', and 'State Secrets Related to National Defence'. Under each heading, the themes receive a pre-defined maximum level of classification and expiry time, for example 'items of information concerning the methods and tactics of the application of witness protection measures, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified as either "top secret" or at a lower level for a maximum period of fifty years.'

The broad categories of information subject to classification enlisted by the U.S. Executive Order are further broken down by agencies to guides issued by originators and tailored to the scope of their activities.[122] The Executive Order requires that the 'agency heads shall complete on a periodic basis a comprehensive review of the agency's classification guidance, particularly classification guides, to ensure the guidance reflects current circumstances and to identify classified information that no longer requires protection and can be declassified'.[123] The same Executive Order also created a Fundamental Classification Guidance Review program in which all federal agencies with significant classification programs had to review their guides. The program resulted in the elimination of several hundred Security Classification Guides.[124]

The Australian guidelines operate with categories of information comparable to the US and also help the originators by providing them a flowchart on how to select an appropriate marking.[125] These guides serve the unification of the classification practice, so that the same type of information should be classified on the same level and for the same duration.

As a rule of thumb, in these systems the secrecy law covers information relvant to all themes which might need protection by classification. That is why no separate provisions for classification in sector-specific legislation are needed, though

regulations governing the work of intelligence agencies may be exceptions. In Sweden, this rule is more concrete as it is permitted to include provisions concerning secrecy in other enactments provided that the Public Access to Information and Secrecy Act makes reference to them. In other words, the Public Access to Information and Secrecy Act must indicate all the instances when official documents are secret.[126]

In case the law does not provide for a unified system of classification, the limits of the classification regime become blurred which may be detrimental to the exercise of freedom of information and expression, and in the long run may harm the rule of law. For example, the Australian Law Reform Commission published a list of more than 150 items on 'provisions in Commonwealth legislation that impose secrecy or confidentiality obligations, *as identified to date.* Provisions that deal only with exceptions to such secrecy or confidentiality obligations and other associated or ancillary matters are not included'.[127]

The limits of classified information may not only be obscured by the abundance of themes of secrets, but also by vague and overly broad provisions. In response to high profile espionage cases in the Russian Federation the Parliamentary Assembly of the Council of Europe invited the Committee of Ministers to:

> 'urge all member states to examine existing legislation on official secrecy and amend it in such a way as to replace vague and overly broad provisions with specific and clear provisions, thus eliminating any risks of abuse or unwarranted prosecutions;
>
> apply legislation on official secrecy in a manner that is compatible with freedom of speech and information, with accepted practices for international scientific co-operation and the work of lawyers and other defenders of human rights'.[128]

5. The protection provided – protective markings and classification levels

What can be classified and why are protective markings needed?

According to the UK Security Policy of 2009, 'when protectively marking a document, it is recommended that a damage or "harm test" is conducted to consider the likely impact if the asset were to be compromised and to help determine the correct level of marking required'.[129] Protective markings have several purposes. First, marking has a practical purpose: it is needed to ensure that adequate protection is provided to information as regards personnel, and physical security. Second, the marking provides information on the level of authority needed for any action to be taken regarding its protection such as reviews of classification, providing access to third parties, etc. Third, markings are defined according to the harm that may occur if information is compromised and criminal sanctions are attached to different levels of classification, which means criminal penalties for compromising classified information are usually proportionate to levels of classification. Furthermore, it is a substantive element of judging criminal offences whether the person compromising the information knew that information was classified – for this reason protective markings have high relevance even to those who generally have no contact with national security matters or classified information.

Practically any phenomenon can be classified as secret. It is very common that *materials* can be classified. For example, in Macedonia (FYR) 'documents, technical devices, any machinery, equipment or separate components thereof or weapons or tools, manufactured or in the process of manufacturing'[130], the Lithuanian rules are even more extensive where '*works* means of scientific, research, testing, draft and technological processes' and 'other objects means materials, liquids, gases, minerals, bacteria and other forms of materials which according to their features or nature, cannot be attributed to the concept of document, product or works'[131]. Often the information does not need to be recorded in any form in order to be protected so can be the spoken word protected in Germany.[132] The Austrian law is very lax as it foresees classification of 'pieces of information, facts, objects and news, independently of its display format and medium' and provides only a non-exhaustive enumeration of the physical forms which can be subject to classification.

The former Estonian law was more careful in this area and delimited the possible classifications of objects; 'a material object shall be marked with a classification marking only if it is possible to obtain a state secret by examining its structure, content or outer surface, by conducting operations with the material object, by testing the material object, or in the course of use or application thereof'.[133] In the United Kingdom, protective markings (classification) 'can be applied to any government assets' however it is a mandatory requirement that assets must be 'clearly and conspicuously marked. Where this is impractical (e.g. a building or physical asset) staff must be made aware of the protective controls required'.[134] It is considerable that the classification of materials – besides the media holding classified information – is not an unavoidable element of a classification system, for example the Czech Republic or Slovenia do not regulate them in their respective secrecy laws.

The classification system of the European Union was altered in line with NATO standards and both comprise four levels of classification: EU Top Secret / EU Secret / EU Confidential / EU Restricted.[135] In the Soviet Union, the traces of whose secrecy regime is still recognisable in many countries of the former Soviet Bloc, the classification system was the following: '[a]ll articles, documents and information are divided into three categories according to the degree of secrecy: 'of particular importance', 'top secret' or 'secret' [reference omitted]. Information 'of particular importance' and 'top secret' constitutes a state secret, and 'secret'

PRINCIPLE 11

a. (a) Whether or not a state has a formal classification process, public authorities are obliged to state reasons for classifying information.
Note: "Classification" is the process by which records that contain sensitive information are reviewed and given a mark to indicate who may have access and how the record is to be handled. It is good practice to institute a formal system of classification, in order to reduce arbitrariness and excessive withholding.

b. The reasons should indicate the narrow category of information, corresponding to one of the categories listed in Principle 9, to which the information belongs, and describe the harm that could result from disclosure, including its level of seriousness and degree of likelihood.

c. Classification levels, if used, should correspond to the levels and likelihood of harm identified in the justification.

d. When information is classified, (i) a protective marking should be affixed to the record indicating the level, if any, and maximum duration of classification, and (ii) a statement should be included justifying the need to classify at that level and for that period.
Note: Providing a statement justifying each classification decision is encouraged because it makes officials pay attention to the specific harm that would result from disclosure, and because it facilitates the process of declassification and disclosure. Paragraph-by-paragraph marking further facilitates consistency in disclosure of unclassified portions of documents.

denotes as official secret'.[136] In some countries, differentiation between state secrets and official or service secrets still lives on and is merged with the four level system, which is further complicated by quasi-secret categories and automatic classification rules. The latter two phenomena are also present in countries without a communist past, while the term 'official secret' has different meanings in the context of official secrets acts.[137] The former Polish secrecy law differentiated between 'state secret' and 'public service secret'; the Lithuanian law has 'state secret' and 'official secret' categories. In the Czech, Hungarian and Macedonian laws, these categories are present only in the transitional provisions as a token of the past regimes.

In case of any review of classification, in addition to justification, it is essential to have basic information available on the fulfilment of formal requirements of the classification procedure. The range of such information may vary from country to country and of course there is other information linked to the classification which has relevance in information management (e.g. reference number) and in protection of information (e.g. number of pages). However, these are not discussed in this paper. The most common requirements from the aspect of formal criteria of classification is the identity of the person classifying the material (originator), so as to verify whether he/she disposes of proper authorisation, the protective marking which refers to the level of classification, and the date and the period of classification in order to define the expiry of classification and the time of regular reviews.[138]

The UK Security Policy points out that '[a]pplying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business' and '[a]pplying too low a protective marking may lead to damaging consequences and compromise of the asset'.[139]

The German regulation warns that the unjustified or over-classification leads to a dilution of the protection of classified information and to the lack of acceptance of the provisions of classification system in general.[140]

In addition, the New Zealand manual stresses the motives for over-classifying as 'genuine doubt about the classification prescriptions, personal uncertainty, a tendency to play safe' and recommends a set of measures to avoid it. Detailed guidance on the correct use of classifications is the most effective, eg. 'standard definitions with up-to-date examples of the correct and incorrect use of classifications, drawn from its own field of activity. The definitions of the security classifications together with the examples should be given to all staff who classify information'. Furthermore '[s]ecurity training should stress the importance of selecting the most appropriate classification. Staff should be reminded that the likely damage caused by unauthorised disclosure is [already] included in the definition of a classification'.[141] According to the German regulation, 'in order to facilitate work and standardise practice, departmental heads may establish classification guidelines for commonly arising cases' – which, in effect, is similar to the list of themes.[142] In Lithuania, in addition to the list of themes, there is security classification guidance, resembling the German guidelines.[143]

It is noteworthy that over-classification is not only relevant for effective information management, but also from a freedom of information perspective: the higher classification the information has, usually the longer it is withheld from the public and the more severe the criminal sanctions for leaking it. Further, the competent authorities may tend to be more reluctant to declassify it.

PRINCIPLE 18

The fact that information has been classified is not decisive in determining how to respond to a request for that information. Rather, the public authority that holds the information should consider the request according to these Principles.

RECOMMENDATION

If there are provisions regarding the classification of potentially non-sensitive materials, there are two important aspects the legislator should keep in mind:
It is a principle of criminal law that the law must be both accessible to, and foreseeable by, anyone so that the individual can know which actions or omissions can make him/her criminally liable. If utterly intangible phenomena may be classified as state secrets, no one can be sure when these phenomena are compromised, which is highly problematic in legal systems which sanction even the unintentional violation of state secrets.
Often it is not practical to classify materials as there are other forms of protection and controls which are also fortified by criminal sanctions.

The issue of over-classification should be addressed both on legislative and practical level.
Effective review mechanisms shall be implemented and the maximum expiry time of classifications shall be limited so that it complies with the principles of proportionality and necessity.
Guidelines should be designed to help originators properly classify information – New Zealand and Germany may serve as good examples. The curricula of trainings should include not only information security, but also freedom of information and other related fundamental rights topics.
Information should be classified on a case by case basis and automatic classification should be avoided, automatic classification rules should be revoked.

6. Access to national security / classified information

What happens when somebody requests access to national security or defence information?

The right and the means of access to information are regulated by FOI acts. In the double act model countries (Chapter 3.1) that have classification/secrecy provisions in acts of the Parliament, there may be further details on access in those instruments. In the single act model countries policies, manuals, regulations and directives may be binding on administrative bodies, and public officials. Yet even though they may provide for means of access, they have no legal effect on rights and obligations of other individuals. As the first prerequisite to gain access, the public body holding the requested information has to be covered by the scope of the FOI Act (see Chapter 9). The second prerequisite is that the requested information is also covered by the scope of the FOI Act. If the public body is not covered by the FOI Act, the requestor may still assert his/her right under international legal instruments or under the constitution – if a constitutional provision on the right to information exists.

In the *double act model* countries, even if the public body is not covered by the FOI Act, the requestor may try to exercise the right of access to information solely under the secrecy act. These acts usually provide for procedures to gain insight into documents, to get acquainted with information – without the right to impart it –, to review and possibly to remove classification by authorised persons. As such, regulations are applicable to any public body within the scope of the secrecy act. In theory, access can be provided, or classification can be removed, and information can be disclosed in conformity with these procedures, though rules of substantial law may be missing.

In the *single act model* countries, if the public body is not covered by the FOI Act, the requestor is in a worse position, as he/she may not even have access to the sublegal rules (guides, manuals, etc.). Even if these rules are accessible, they often completely disregard everything external to the public bodies that are using classified information.

Further, if there is an FOI act which provides for access to information, then that information can only be withheld if it falls under an exemption. Nevertheless, protective measures on sensitive information are independent of the FOI exemption and vice versa, which means the two systems can exist next to each other without having any point of connection. This situation is clearly visible in the interpretation of the New Zealand law: 'Classifications alone do not justify withholding official information. All requests for information, regardless of classification, must be considered using the criteria in the Official Information Act 1982'.[144] According to the Australian law 'the classification markings on a document (such as 'secret' or 'confidential') are not of themselves conclusive of whether the exemption applies'.[145] In the United Kingdom's Security Policy Framework of 2009 the following interpretation was present

> '[t]he Freedom of Information Act 2000 (FOIA) gives any person the right to request and be provided with information held by public authorities, although exemptions apply to specific information as defined by the Act. Whilst FOIA makes no reference to the Protective Marking System, protective markings may be a helpful indicator that an exemption applies. However, the presence, or absence, of a protective marking is not the deciding factor as to whether information should be released or not under FOIA'.[146]

Accessibility of information	Not classified	Classified
Not exempted under FOI Act	public	originally illegal or obsolete classification; public interest override
Exempted under FOI Act	other protection is provided or should be provided	genuine (state) secret

Later interpretation on how laws and sublegal documents have to read together was revoked, as the Security Policy Framework 'is not intended to provide legal guidance. Departments will need to take legal advice on a case by case basis in relation to information law (including on the Freedom of Information Act 2000(...)'.[147]

In the Minimum Security Standards of the Republic of South Africa it is explained:

> 'The mere fact that information is exempted from disclosure in terms of the Open Democracy Act, does not provide it with sufficient protection. Such information will always be much sought after by certain interest groups or even individuals, with sufficient access to espionage expertise, and highly sophisticated technological backing. […]
>
> Where information is exempted from disclosure, it implies that security measures will apply in full. This document is aimed at exactly that need: providing the necessary procedures and measures to protect such information. It is clear that security procedures do not concern all information and are therefore not contrary to transparency, but indeed necessary for responsible governance'.[148]

Though this provision may seem clear, the legal framework is much more complicated. 'The constitutional right of access to information coexists uneasily with the laws and administrative instruments designed to protect classified information'[149] as the Protection of Information Act of 1984 (apartheid-era successor of the Official Secrets Act) and the Minimum Information Security Guidelines (which builds on apartheid era administrative instruments) have to be applied together with the Promotion of Access to Information Act. It is not an easy task as the legislation has failed harmonised these rules so far.

The German law is slightly different in this sense as the relationship between the two systems are better defined. The federal FOI Act lists among its exemptions 'where the information is subject to an obligation to observe secrecy or confidentiality by virtue of a statutory regulation or the general administrative regulation on the material and organisational protection of classified information, or where the information is subject to professional or special official secrecy'.[150] Furthermore, the federal act on vetting procedure prescribes that sensitive information has to be classified and also defines the levels of classification. However, details of the classification system are regulated in an administrative document.[151]

Two variables of freedom of information and classification are indicated in Table 1. Any information requested will fall into one of the four categories. In case of public information, the only question is whether it is already published or has to be disclosed on request. Illegal or obsolete classifications should be reviewed (Chapter 11.1 and 11.2), but in case of a public interest override, information may also fall into this category (Chapter 4.2) and the classification has to be reviewed as well. Information that is exempted under FOI but not classified may be protected by other means (e.g. business secrets)[152] depending on the legal system. Alternatively, it could not be classified due to an omission or oversight by the public body holding the information. In the latter case, a review would be needed. The last option is that information is exempted for the protection of public interest (and there is no other public interest that would outweigh the one which enjoys the protection) and adequately classified.

On the whole, in either model a request can have the following results: 1. access or partial access may be provided to the requestor at full disposal of the received information, 2. access or partial access may be provided without the rights of use or distribution, 3. access may be refused, 4. a 'neither confirm nor deny' answer is given.

6.1 ACCESS AND THE PRINCIPLES OF *NEED TO KNOW* AND *RIGHT TO KNOW*

It is a common feature of classification regimes that the principles of *personnel security*[153]*, need to know and originator control* must be applied overall in the management of information, including responding to information requests.

Alasdair S. Roberts describes these principles in the context of NATO, but they are present practically in all classification regimes.

> 'The first of these is "the NEED TO KNOW principle": that individuals should have access to classified information only when they need the information for their work, and access should never be authorized "merely because a person occupies a particular position, however senior." This is regarded as a "fundamental principle" of security. Judgments about whether an individual has a "need to know" are made by the originator of the document, or by one of the addressees identified by the originator.
>
> The second rule that restricts the distribution of information might be called the principle of originator control. The principle acknowledges the right of member states, and NATO itself, to set firm limits on the distribution of information that is circulated among member states. […]
>
> The parties to the North Atlantic Treaty . . . will make every effort to ensure that they will maintain the security classifications established by any party with respect to the information of that party's origin; will safeguard accordingly such information; . . . and will not disclose such information to another nation without the consent of the originator'.[154]

In the *double act model* countries, it is a common characteristic of the secrecy acts that the public body holding classified information has the authority to grant access. In these cases, laws customise the application of these principles to different situations.
At the same time in the *single act model* countries, the FOI acts may remain silent on the issues of classification and on the three above mentioned principles while the policies, manuals, regulations, directives on protection of classified neither offer clear

instructions concerning public disclosure.

The below examples do not refer to details of the application of personnel security, need to know and originator control principles. However, the following provisions show that these principles govern the cited secrecy laws when they provide access, or partial access, to individuals exercising their right of access to information.

Provisions on the legal basis for the access to state secrets in the Estonian law is a good example for the application of these principles: '1) by virtue of office; 2) under the decision of a head of an agency; 3) under a Personnel Security Clearance; 4) in relation to the adoption of witness protection measures or 5) by the ruling of an investigation institution, prosecutor's office or court'.[155] Of course conditions for providing access are further detailed and the extent and level of access, as well as requirements of confidentiality, are clearly defined in the spirit of 'need to know'. Similarly, in Poland there was a provision that stated 'when exceptional circumstances so warrant, certain persons or institutions may be given access to classified information with the status of a state secret under a written authorisation'.[156]

A particular area of the application of the need to know principle is the intersection of classification rules and of the rules of court procedures. The latter rules have to reconcile the requirement of adequate protection of classified information and the right to fair trial. This exercise rests with the investigative authorities, the prosecutor's office or the court (depending of the legal system and the actual phase of the legal procedure) which are authorised by law to issue a ruling on access to classified information with regard to the actual legal procedure.[157] Such provisions are substantiated by the relevant criminal, administrative, etc. procedural laws.[158] Occasionally, not only do the procedural laws refer to classification rules, but the secrecy laws also contain references to procedural laws for example in Austria, Czech Republic, Hungary, Macedonia (FYR) and Poland. It appears that public interest in sound functioning of the public administration, in fair trials, in protection of witnesses and in numerous other matters (that are occasionally left to the discretion of the originators) is important enough that the legislator enables access to classified information. However, public interest in these fields is still embraced by the principle of need to know which is contrary to the right to know.

Information security considerations appear to dominate the assessed secrecy regulations (with the exception of the Mexican one where the same law provides for freedom of information). These considerations can be boiled down to the following requirements which are well summarised in a security policy of the NATO:

> 'to achieve adequate security protection of NATO classified information handled in systems, a balanced set of security measures (physical, personnel, information and INFOSEC) shall be identified and implemented to create a secure environment in which a system operates, and to meet the following security objectives:
> (a) to ensure the confidentiality of information by controlling the disclosure of, and access to, NATO classified information, and supporting system services and resources;
> (b) to ensure the integrity of NATO classified information, and supporting system services and resources; and
> (c) to ensure the availability of NATO classified information, and supporting system services and resources'.[159]

A similar approach is codified in the security rules for protecting EU classified information (EUCI)

> 'Risk to EUCI shall be managed as a

> process. This process shall be aimed at determining known security risks, defining security measures to reduce such risks to an acceptable level in accordance with the basic principles and minimum standards set out in this Decision and at applying these measures in line with the concept of defence in depth as defined in Appendix A. The effectiveness of such measures shall be continuously evaluated'.[160]

These two regulations demonstrate that the aim of law and policymakers is to make sure that the system of protecting classified information is watertight. This means that all individuals having contact with classified information or media have to be recorded and all risks have to be assessed. If a public body provides access to an individual under the circumstances that s/he has a justified need to know and has undergone security vetting, which came back clean, then that person would still be required to pledge in writing that the information will remain in confidence – in line with the security requirements. This means that the individual is not allowed to impart by any means, to anyone what s/he learned, otherwise the individuals having knowledge of the secret could not be identified. Nevertheless, since the nineties, not only in the United States

> 'there has been a growing recognition of the need to replace a risk avoidance approach to security, which seeks to anticipate all risks in the protection of assets, with a risk management approach, which seeks to concentrate limited resources on those assets the loss of which would have the most profound effect on the national security'.[161]

This process has, by no means, been shared by all countries assessed in this study and even the US has seen serious reversions in this field. All in all, this thinking is still very far from the core principles of the right to freedom of information which clearly includes the freedom to seek, receive and impart information.

Sweden provides an interesting example of regulation both for the need to know and for the white space that exists between the *need to know and right to know.*

> 'Secrecy does not for instance prevent information being made available to another authority or to a private party, if it is necessary in order for the authority to perform its own functions. Thus, if it is necessary, an authority may, for example, consult an independent expert, even if this should involve providing information to the expert that is subject to secrecy'.[162]

> 'An authority may not demand that a person who wishes to obtain an official document identifies himself or herself or state what the document is to be used for. However, if it relates to a document falling under one of the provisions of the Public Access to Information and Secrecy Act, the authority must sometimes know who wishes to obtain it and what it will be used for. Otherwise, the authority might not be able to make a decision concerning whether the document may be made available. In that event the applicant may either say who he or she is and state what the document will be used for (for example, research) or relinquish any possibility of obtaining it. An authority has, under certain circumstances, the possibility of providing a document subject to conditions (‘reservations’) restricting the applicant’s right to use the information contained within the document.
> The authority may, for example, forbid the applicant to publish the information or to use it for purposes other than research'.[163]

In essence access, or partial access, to information may be provided either on the

basis of need to know or on the basis of right to know, though the formula and the results are very diverse.

6.2 PARTIAL ACCESS

Although security measures can be applied to electronic hard drives, disks, paper files and other similar items[164] holding the classified information, it is crucial to understand that in a document, or set of information, not every piece needs classification or in fact is classified. When requesting information the public body holding the classified information should separate the classified information from the non-classified information whatever the medium for holding it may be. This is something which is normally prescribed in national FOI rules and is confirmed as good practice by the Council of Europe Convention on Access to Official Documents.[165] The manual of New Zealand prescribes 'in complex documents such as books, reports, memoranda or minutes of meetings, separately classify each chapter, section, page or paragraph; this can be indicated by inserting the appropriate classification in parentheses immediately following the section or paragraph number or in the sideline if unnumbered'.[166] The Executive Order of the United States prescribes that 'with respect to each classified document, the agency originating the document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are unclassified' and 'the classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form'.[167]

PRINCIPLE 22

Exemptions from disclosure apply only to specific information and not to whole documents or other records. Only specific information for which the validity of a restriction has been demonstrated ('exempt information') may be withheld. Where a record contains both exempt and non-exempt information, public authorities have an obligation to sever and disclose the non-exempt information.

However, it may also be the case that exempt and nonexempt information cannot be separated. According to the Department of Justice Guide to the Freedom of Information Act in the US, 'the statutory standard requires agencies to release any portion of a record that is nonexempt and that is "reasonably segregable" from the exempt portion', furthermore it notes (based on extensive jurisprudence of courts) that 'segregability should not be determined based on an evaluation of whether nonexempt portions of documents would be "helpful" to the requester if segregated and released', although 'when nonexempt information is "inextricably intertwined" with exempt information, reasonable segregation is not possible'. The Guide continues 'segregation is not reasonable when it would produce "an essentially meaningless set of words and phrases," such as "disjointed words, phrases, or even sentences which taken separately or together have minimal or no information content"' and it also refers to a case where '"any disclosable information is so inextricably intertwined with the exempt, confidential information that producing it would require substantial agency resources and produce a document of little informational value" finding that because agency would require eight work-years to identify all nonexempt documents in millions of pages of files, very small percentage of documents that could be released were not "reasonably segregable"'.[168]

There are two further important rules relevant to partial access. Even if classified and non-classified information are separated, other exemptions may still apply

and, as a result, such exempted information has to be further protected (see Chapter 12 on overlapping secrets). [169]

The other one is a wide-spread rule that leads to the mosaic theory: files or groups of documents must be protected to the standard required for the highest marked document contained within it; 'Compromise of aggregated or accumulated information of the same protective marking is likely to have a higher impact (particularly personal data). This should not generally result in a higher marking but may require additional handling arrangements. If the accumulation of data results in a more sensitive asset being created, then a higher protective marking should be considered'.[170]

6.3 MOSAIC THEORY

The provisions concerning the *'separation of different classifications is possible' and 'highest classification rules the document'* were further refined in different legislations which lead to the mosaic theory.

'The 'mosaic theory' describes a basic precept of intelligence gathering: Disparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information. Combining the items illuminates their interrelationships and breeds analytic synergies, so that the resulting mosaic of information is worth more than the sum of its parts'.[171] So as to counter the risks posed by the mosaic, a number of laws prescribe that 'classified information (and) materials, in particular documents or collections of documents, shall be accorded a secrecy classification equal to or higher than that given to the highest-rated information or, as applicable, the highest-rated document in the collection of documents' or contain similar rules.[172]

A similar approach can be found in the NATO Security Policy: 'when information from various sources is collated the product shall be reviewed for overall security classification since it may warrant a higher classification than its component parts'.[173] According to EU rules, 'when information from various sources is collated, the final product shall be reviewed to determine its overall security classification level, since it may warrant a higher classification than its component parts'.[174] The provision, which requires classification of the highest-rated documents applied to all parts of the file, does not mean the application of mosaic theory. It is only the result of precautionary measures to protect the most sensitive information. However, the mosaic approach is demonstrated in cases where higher classification is provided to some of the information than its component parts.

The Australian law also recognises the mosaic theory and its guidelines refer to several cases in which it was claimed that cumulatively disclosed information would add up to sensitive information. At the same time, the Australian Information Commissioner also warns that 'the mosaic theory does not relieve decision makers from evaluating whether there are real and substantial grounds for the expectation that the claimed effects will result from disclosure. It is a question of fact whether the disclosure of the information, alone or in conjunction with other material, could reasonably be expected to enable a person to ascertain the identity or existence of a confidential source. This is not always simple. For example, in Re Slater and Cox the evidence that persuaded the AAT of a 'mosaic effect' claim was an analysis of 22 thirty-five-year-old documents'.[175]

In the case of Vereniging Weekblad Bluf! v. the Netherlands, the ECtHR stated that 'it is open to question whether the information in the report was sufficiently sensitive to justify preventing its distribution. The document in question was six years old at the time of the seizure. Further, it was of a fairly general nature, the head of the security service having himself admitted that in 1987 the various items of information,

taken separately, were no longer State secets'.[176]

It is worth noting that the Republic of South Africa standards call into question this approach as 'every document must be classified on its own merit (in accordance with its own contents) and in accordance with the origin of its contents, and not in accordance with its connection with or reference to some other classified document'. The only exception regarding this rule is when this document contains a reference to the existence of another classified document, which in turn refers to a third piece of classified information.[177]

6.4 DUTY TO CONFIRM OR DENY

When someone files an information request and receives an answer, one would expect that either the information is provided or the request is refused and the refusal is accompanied by some reasoning on why the information cannot be disclosed. In fact, there is a third possibility; when the requested authority declares that it cannot either confirm or deny that the sought piece of information exists. Although perhaps the most Kafkaesque element of any classification system is when even the existence of a secret (a piece of information) is a secret - yet this restriction is sometimes necessary.[178] In these cases, references to classified information have to be classified. If someone requests such information, the public body holding the information is not required to confirm or deny the existence of the requested information. The same rule applies to pro-active disclosure: public registers shall not contain reference to such information. For example, the registers of the European Parliament, Council and Commission may refer to sensitive documents, but there could be sensitive documents which are not officially recorded (non-papers).[179]

'Neither confirm, nor deny' refusals may be appropriate in cases when even the knowledge of the existence of some information would endanger the public interest. Such is the case when a criminal is investigated or secretly observed and the disclosure of the fact that he/she is under suspicion would obstruct the investigation.

PRINCIPLE 19

a. Upon receipt of a request for information, a public authority should confirm or deny whether it holds the requested information.

b. If a jurisdiction allows for the possibility that, in extraordinary circumstances, the very existence or non-existence of particular information may be classified in accordance with Principle 3, then any refusal to confirm or deny the existence of information in response to a particular request should be based upon a showing that mere confirmation or denial of the existence of the information would pose a risk of harm to a distinct information category designated in a national law or regulation as requiring such exceptional treatment.

The FOI Act of the United Kingdom distinguishes two duties related to the right of access to information: '(a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and (b) if that is the case, to have that information communicated to him'.[180] If the public body holding the information neither confirms, nor denies its existence, it means refusal to provide information according to both of the articles discussed above.

The UK Information Commissioner however makes it clear that

'When a public authority refuses either

> to disclose requested information or confirm or deny that that information is held, it must issue a refusal notice stating the fact of refusal, the exemption used and why the exemption applies. A public authority should be clear in its refusal notice that where the public interest test applies, it has applied it in relation to each duty individually'.[181]

The Information Commissioner also gives further guidance on 'neither confirm, nor deny' refusals in national security matters:

> 'In order to be effective, such a policy should be applied consistently to requests for certain types of information, both when the information is held and when it is not. However, the authority should always ascertain what information (if any) it holds and examine it in order to determine what exemptions may apply. The 'neither confirm nor deny' response can only be given if any information held is exempt'.[182]

Other legislations, such as the Hungarian, do not differentiate between the duties of providing information, whether the authority holds the requested information and the actual provision of the requested information. In Lithuania, the definition of classified information states that 'information concerning the existence of documents' can be classified too.[183]

Australia, New Zealand[184], Slovenia[185] and the United Kingdom[186] have separate provisions on the duty to confirm or deny. The FOI Act of Australia states that 'nothing in this Act shall be taken to require an agency or Minister to give information as to the existence or non-existence of a document where information as to the existence or non-existence of that document'[187] and documents affecting national security, defence, international relations, enforcement of law and protection of public safety can be withheld and the 'agency may instead give the applicant notice in writing that it neither confirms nor denies the existence of the document. Yet if the document existed, itwould be exempt'.[188]

RECOMMENDATION

In case of a 'neither confirm, nor deny' refusal – as the UK legislation provides for – the authority should communicate the fact of refusal, the exemption used and why the exemption applies.

Public interest tests should also be applied in internal and external review mechanisms so as to avoid arbitrary application of 'neither confirm, nor deny' denials.

7. Justification of restricting right of access to information

The present chapter describes how the onus is not on the requestor to provide reasons for disclosure, but on public authorities to justify non-disclosure.

In any country – which includes 167 Parties of the International Covenant on Economic, Social and Cultural Rights[189] – where freedom of information is recognised as a constitutional right or as a human right, the legislation has to balance between the free exercise of the right and the public interests that may put limitations on it. As freedom of information is a right and not a favour or discretion granted by an authority, the burden of proving the necessity and proportionality of any restriction lies with the authority aiming to restrict it, regardless of the nature of information. **Principle 4** describes it with the following terms:

a. 'The burden of demonstrating the legitimacy of any restriction rests with the public authority seeking to withhold information.

b. The right to information should be interpreted and applied broadly, and any restrictions should be interpreted narrowly.

c. In discharging this burden, it is not sufficient for a public authority simply to assert that there is a risk of harm; the authority is under a duty to provide specific, substantive reasons to support its assertions.
Note: Any person who seeks access to information should have a fair opportunity to challenge the asserted basis for a risk assessment before an administrative as well as a judicial authority, consistent with Principles 26 and 27.

d. In no case may the mere assertion, such as the issuing of a certificate by a minister or other official to the effect that disclosure would cause harm to national security, be deemed to be conclusive concerning the point for which it is made.'

It is a general principle which is present in almost all freedom of information systems that in case an information request is refused, the burden of proof lies with the authority that holds the information requested. Alongside the criteria of necessity and proportionality, it is an indispensable element of the restriction of any fundamental right, including the right of access to information, that the individual concerned shall know why the restriction was needed and in which manner it serves any legitimate aim. As the UN Human Rights Committee emphasised, '[a]uthorities should provide reasons for any refusal to provide access to information'.[190]

In the practice of the ECtHR on Article 6 of the European Convention on Human Rights (hereinafter: ECHR) 'the Court has frequently held that the reasoning provided in court decisions is closely linked to the obligation to ensure a fair trial as it allows the rights of the defence to be preserved. Such reasoning is essential to the very quality of justice and provides a safeguard against arbitrariness'.[191] Nevertheless, the criteria of a fair trial enshrined by Article 6 should not be limited to criminal proceedings and not even to proceedings of courts.[192] As classification may result in non-disclosure of requested information, it is crucial to provide written justification on why the right of access to information has to be restricted, as this is the only way to prevent arbitrary classifications. At the same time, it is not an otherwise unnecessary exercise which is only needed to satisfy fair procedure concerns. Justifications may reduce over-classification that saves resources of the agencies handling classified information.

Justification is proof of whether information was classified as a result of a proper harm (and public interest) test and the decision-maker was able to explain 'the factual and rational bases on which the exemptions rest'.[193] The justification helps the authority to perform internal reviews on classification. Having a justification also

enables bodies performing external reviews (such as information commissioners) to indirectly assess the formal and substantive criteria of the classification – even in cases where they are not authorised to access the information directly.

On a practical level, as information requests are regulated by freedom of information laws, the first level of assessment will be based on these laws and therefore this principle has to be applied in line with the FOI law. The second level of application concerns the classification procedure (Chapter 4). Though classification procedures may contain harm and public interest tests, which provide for balancing between disclosing and withholding information, a subsidiary principle on doubts may still help the originators.

7.1 CERTAINTY AND DOUBTS IN ASSESSING CLASSIFICATION

Executive Order 13526 (Classified National Security Information of the United States) applies rules concerning doubts in classification with caveats regarding the substantive basis of withholding information: 'If there is significant doubt about the need to classify information, it shall not be classified. This provision does not: (1) amplify or modify the substantive criteria or procedures for classification; or (2) create any substantive or procedural rights subject to judicial review.'[194]

Section 33 of the Australian Freedom of Information Act (1982), which deals with documents affecting national security, defence and international relations, has the following provision:

'A document is an exempt document if disclosure of the document under this Act:

- **a.** would, or could reasonably be expected to, cause damage to:
  - **ii.** the security of the Commonwealth;
  - **iii.** the defence of the Commonwealth; or
  - **iv.** the international relations of the Commonwealth;'

The Australian Freedom of Information Guidelines of 2009 (which preceded the guidelines of the Office of the Australian Information Commissioner)[195] commented that 'The decision-maker must have real and substantial grounds for the expectation that harm will occur and must not rely on grounds which are merely speculative, imaginable or theoretically possible. (...) Something which is *reasonably expected* is an expectation that is based on reason, one for which *real and substantial grounds* exist when looked at objectively which are not irrational, absurd or ridiculous or fanciful, imaginary or contrived. Decision-makers must keep in mind that they are considering the reasonableness of the expectation of the alleged effect, not the reasonableness of the claim for exemption'.[196]

7.2 THE FORM OF ASSESSING THE NEED FOR CLASSIFICATION

In line with above requirements, the Slovene law prescribes that '[t]he assessment on the basis of which information is given the level of classification shall be in written form'.[197] The German rules also prescribe that it must be coherently demonstrated which threats, harms or other disadvantages can concretely stem from unauthorised access. Principally, external security, foreign relations, internal security and the interests of third parties which need to be protected by Germany (endorsed by the highest authority responsible) should be assessed. Although there is no clear indication that the assessment should be in written form, the complexity of the question and other provisions of the regulation indicate so.[198] According to the Mexican law, both the document containing the classified information, and an index, have to comprise the grounds for classification, though it does not necessarily mean a detailed justification.[199] The Hungarian law also regulates that the justification has to contain among other matters, the specific subject to which the information pertains (see Chapter

4.3) and the facts and circumstances which require the classification.[200]

7.3 CERTIFICATES

'The issuing of ministerial certificates in order to claim public interest immunity was common in the United Kingdom and Australia until the 1960s. In 1942, the House of Lords made a controversial decision – in the context of a world war – that courts should accept without question a certificate issued by a minister certifying the Government's view that the document or secret should be excluded in the public interest'. In the UK, this doctrine was overturned in 1968 and 'a minister's certificate was no longer able to protect information in and of itself, and that a trial judge had to balance the state interest against the broader public interest'– the approach has continued since.[201] Conclusive certificates are enacted in the UK FOI Act 2000. A Minister of the Crown can issue conclusive certificates among others to exempt information that is related to bodies of national security competence (section 23(2)), for the purpose of safeguarding national security (section 24(3)). 'A certificate does not have to refer to a specific request or to specific information that is held. It can refer to a category of information and can apply to future requests'.[202] If a conclusive certificate is issued, the Information Commissioner cannot undertake a merit review of the public authority's decision of non-disclosure.[203] The applicant, or the Commissioner, may appeal to the Tribunal against the certificate (section 60 of the UK FOI Act). In the UK FOI Act there is another certificate, which may be issued against the decision notice of the Commissioner, in exceptional cases, in which an accountable person related to that authority states that, for reasonable grounds, the exemption had to be applied (section 53(2)). In the case of disclosure of Cabinet minutes concerning military action against Iraq, a certificate under section 53(2) was issued. The practical effect of the certificate was to overrule the Tribunal's decision, which caused a huge public uproar after years of legal battles in the United Kingdom.[204]

In Australia, until October 2009, the following rule was in force: 'once a Minister issues a conclusive certificate under the Australian Federal Act review on the merits is obviated. The matter then proceeds only on whether the Minister had reasonable grounds for the claims made in the certificate. If the AAT [Administrative Appeals Tribunal] decided there was no reasonable grounds the Minister might still decide not to revoke the certificate and instead report that decision to parliament'.[205] In this case, public interest in withholding information did not have to be weighed

RECOMMENDATION

Justifications of classification are essential both for internal and external reviews. The legal basis and substantive grounds for the restriction of access are contained in these documents, which enable the reviewer to assess the necessity and legality of classification. At the same time, the obligation of producing justification requires the originator to consider the possible harm of unauthorised disclosure and the level of protection needed to safeguard the information.

In order to set up effective review mechanisms, written justifications should be required on all levels of classification, which contain all details of classification, so as to enable a review on whether the classification is formally and substantively correct.

As a main rule, 'basic information' and justification themselves may not be classified so as to provide a baseline to anyone asking for reviews of classification and seeking legal remedies within the ambit of their right of access to information.

against public interest in disclosing it, unlike in the procedure of the UK Commissioner. In 2009, Australia repealed its FOI provisions on conclusive certificates.[206] As a result, no public body has the power to issue conclusive certificates and the Administrative Appeals Tribunal 'may undertake full merits review of all exemption claims in the normal manner. The Certificates Act provides that existing conclusive certificates will be revoked on and from the time a new request for access to a document covered by a certificate is received on or after commencement of the Act'.[207]

The Official Information Act of New Zealand also has a section on *Conclusive reasons for withholding official information* which covers, among others, information on matters of defence, national security and foreign relations.[208] When this section is applied, 'there is no requirement to consider whether the interest in withholding is outweighed by countervailing public interest considerations. Effectively, the Act deems it to be in the public interest for information to be withheld where the requirements of section 6 have been met'.[209] Making the information the 'would be likely to prejudice the security of defence of New Zealand' available, would have to be assessed on case by case basis, but no public interest test has to be performed. Where the Prime Minister certifies that the making available of any information would be likely to prejudice, for example, the security or defence of New Zealand, or the international relations of the Government of New Zealand, 'an Ombudsman shall not recommend that the information be made available, but may recommend that the making available of the information be given further consideration by the appropriate department or Minister of the Crown or organisation'.[210] Since the Ombudsman cannot recommend the disclosure of the information, there is no certificate in place that would be similar to the UK. According to the Review of Official Information Act 1982 and Local Government Official Information Act 1987 no legislative change is foreseen in this area.[211]

7.4 QUASI-SECRETS

There is a grey zone between classified information and information accessible to the public. These are often given designations such as 'for official use only', 'sensitive but unclassified' or 'confidential'. This study cannot attempt to explore why the grey areas exist, but its rough outlines can be given.[212] There is a vast amount of information which does not genuinely fall under any exemption, but which public officials are nonetheless reluctant to disclose. It might be possible that some pieces would fit in categories of classified information, if exemptions are interpreted in a lax manner. Yet classification is complicated, time-consuming, and expensive. Further, such classification would possibly fail at the harm test.

Still, the public officials may look for a legal basis to withhold it from the public, sometimes for reasonable grounds, sometimes only for their convenience.

Undoubtedly, public officials need a 'space to think' – protection against premature disclosure of their opinion in decision-making procedures. It is also recognised by Article 3 of the Council of Europe Convention on Access to Official Documents, as 'each Party may limit the right of access to official documents. Limitations shall be set down precisely in law, be necessary in a democratic society and be proportionate to the aim of protecting: (...) the deliberations within or between public authorities concerning the examination of a matter'. However, the scope of quasi-secrets goes far beyond this objective by virtue of the different vague categories present in almost every freedom of information system.

In the United States, there were more

than 100 different policies for such information across the Executive branch that requires protection, yet was not classified. 'This ad hoc, agency-specific approach has created inefficiency and confusion, leading to a patchwork system that fails to adequately safeguard information requiring protection, and unnecessarily restricts information sharing by creating needless impediments'.[213] To manage their grey zone, President Obama issued the Executive Order 13556 'Controlled Unclassified Information' in 2010, but its results are not visible yet as of the beginning of 2013.[214]

In Macedonia (FYR), '[t]he information not intended for public use, the disclosure of which would result in decreased efficiency of the work of the state bodies, shall be marked with FOR LIMITED USE'.[215] In Estonia, there is a category of 'information intended for internal use'.[216]

The exemptions of the FOI Act of the United Kingdom cover nearly every imaginable risk (and more than a few unimaginable ones). However, consistent with its precautionary approach, the *sub-national security marking* PROTECT was introduced. 'Any material originating outside of government, that is not covered by a recognisable protective marking, international agreement, contract or other arrangements, but is marked in such a way to indicate sensitivity, must when handled by HMG, be protected to at least the level offered by the PROTECT marking, and a higher marking should be considered'.[217] New Zealand has two categories in this zone '[s]ecurity classifications for material that needs to be protected because of public interest or personal privacy are: IN CONFIDENCE *(reference omitted),* SENSITIVE *(reference omitted)*'.[218] Still, classifications alone do not justify withholding official information. All requests for information, regardless of classification, must be considered using the criteria in the 'Official Information Act 1982' and the same logic applies to the UK sub-national security marking as well.[219]

On the other hand, there are few examples of contrary tendencies. In 2004, the Hungarian Constitutional Court rendered a decision in which it found that categories

> 'related to the preparation of decision-making' and 'created for internal use' are vague, and the application of these unclear concepts may result in the arbitrary restriction of the publicity of data of public interest.(...) The conceptual vagueness, lack of differentiation and joint use of the expressions 'data created for internal use' and 'data related to the preparation of decision-making', as well as the application of the same rules thereto constitute – in themselves – such a serious regulatory deficiency that results in the unnecessary and disproportionate restriction of the constitutional fundamental right to the publicity of

> data of public interest [reference omitted], because the categories of data to be excluded from publicity are vague.'[220]

In line with this decision, the Parliament detached the 'decision-making' information from 'internal use' information and abolished the latter category.[221] Sweden tries to eliminate the grey zone by a rule which states that, '[n]otation other than the word "secret" may not be used. Thus, expressions such as "in confidence", "confidential" or "for official use only" must not be used'.[222]

RECOMMENDATION

There should be a clear distinction in every legislation between the classification regimes and other measures to the effect of withholding information.

It should be avoided that the legal protection provided to protect classified information, and the resources allocated to safeguard them, are used to withhold quasi-secrets from the public.

If no concrete and legitimate interest exists in classifying information or the information falls under an exemption established by an act of the Parliament, then that information should be available to the public.

'Internal use', 'decreased efficiency' and other vaguely worded terms do not comply with a rule of law system, therefore these definitions should be repealed. Hungary and Sweden may provide good examples in this area.

8. Prohibited classifications and information of public interest

Two sides of the same coin – prohibitions on non-disclosure and provisions on presumption of (proactive) disclosures are detailed below.

While the freedom of information law fleshes out the configuration of power, prohibitions are what reveal the most about a country. These prohibitions of non-disclosures can be found both in FOI Acts and secrecy laws. Concurrently, there is a legitimate public interest in proactive publication of certain categories of information even if they are related to national security.

Principle 10 stipulates that some categories of information are subject to 'a very strong presumption, and in some cases an overriding imperative, that such information should be public and proactively disclosed. Information in the following categories should enjoy at least a high presumption in favor of disclosure, and may be withheld on national security grounds only in the most exceptional circumstances and in a manner consistent with the other principles, only for a strictly limited period of time, only pursuant to law and only if there is no reasonable means by which to limit the harm that would be associated with disclosure'. (see Annex III: Categories of Information with a High Presumption in Favour of Disclosure or Overriding Interest in Favour of Disclosure).

The Swedish standard is the most simple: '[o]fficial documents may not be kept secret in order to protect interests other than those listed' in Chapter 2 Article 2 of the Freedom of the Press Act.[223] Although this requirement seems to be obvious, and it is implicit in every FOI law, it still, on occasion, may be needed to remind public officials that are holding the requested information. It should also be evident that there is no public interest in covering up wrongdoings by classification. Still FOI systems are not perfect, and thus often clear prohibitions have to be in place to make this rule concrete. In 1972, in the United States prohibitions were introduced since 'the controls which have been imposed on classification authority have proved unworkable, and classification has frequently served to conceal bureaucratic mistakes or to prevent embarrassment to officials and administrations'.[224] These rules served as a blueprint for similar legislations in numerous countries such as Australia.[225] Currently in the U.S. (a) 'in no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:

1. conceal violations of law, inefficiency, or administrative error;

2. prevent embarrassment to a person, organization, or agency;

3. restrain competition; or

4. prevent or delay the release of information that does not require protection in the interest of the national security.

b. Basic scientific research information not clearly related to the national security shall not be classified'.[226]

Mexico's law is best known for three innovative characteristics in this field. First, it explicitly states that none of the law's exemptions apply to information necessary for

> 'investigating grave violations of fundamental rights or crimes against humanity'. This establishes a *blanket public interest override* for all information related to delicate issues such as political assassinations, the persecution of ethnic minorities or government censorship of the press. The information must be made public even in cases where it would arguably affect 'national security' or any other State interest included in Articles 13 and 14'.[227]

The grave violations of fundamental rights or crimes against humanity are defined as

'those serious breaches of fundamental rights and crimes against humanity shall be considered, as established in the treaties ratified by the Senate of the Republic or in the resolutions issued by international organizations recognized by the Mexican State as competent, as well as in the applicable legal provisions'.[228]

The UN Human Rights Council's joint study on secret detention found in its conclusions that

> 'The evidence gathered by the four experts for the present study clearly shows that many States, referring to concerns relating to national security - often perceived or presented as unprecedented emergencies or threats - resort to secret detention. […] Secret detention as such may constitute torture or ill-treatment for the direct victims as well as for their families. As many of the interviews and cases included in the present study illustrate, however, the very purpose of secret detention is to facilitate and, ultimately, cover up torture and inhuman and degrading treatment used either to obtain information or to silence people'.[229]

Based on the conclusions of the study they put forward the recommendation that

> 'Secret detention should be explicitly prohibited, along with all other forms of unofficial detention. Detention records should be kept, including in times of armed conflict as required by the Geneva Conventions, including with regard to the number of detainees, their nationality and the legal basis on which they are being held, whether as prisoners of war or civilian internees. […] All steps necessary to ensure that the immediate families of those detained are informed of their relatives' capture, location, legal status and condition of health should be taken in a timely manner'.[230]

The recommendations are unambiguous: even in cases of seemingly unprecedented national security threat detention records should be kept and the immediate families of those detained have to be informed of details of the detention. These requirements show a clear prohibition of withholding national security information. Since detention is not a personal matter, it cannot be exclusively understood as a question of right to informational self-determination or right to fair trial. Rather it has to be considered as a freedom of information issue as well.

In Slovenia and Macedonia (FYR) the classification of information which covers 'criminal offence, the exceeding or abuse of authority, or some other unlawful act or behaviour' is invalid.[231] The Information Security Standards of the Republic of South Africa note that 'Security measures are not intended and should not be applied to cover up maladministration, corruption, criminal actions, etc., or to protect individuals/ officials involved in such cases'.[232]

The Estonian FOI Act contains a list of 'prohibition on classification of information as internal'. It comprises a set of diverse themes:

> '1) results of public opinion polls; 2) generalised statistical surveys; 3) economic and social forecasts; 4) notices concerning the state of the environment; 5) reports on the work or the work-related success of the holder of information and information on the quality of the performance of duties and on managerial errors; 6) information which damages the reputation of a state or local government official, a legal person in private law performing public duties or a natural person, except private personal data; 7) information on the quality of goods and services arising from protection of the interests of

consumers; 8) results of research or analyses conducted by the state or local governments or ordered thereby, unless disclosure of such information would endanger national defence or national security; 9) documents concerning the use of budgetary funds of the state, local governments or legal persons in public law and remuneration and compensation paid from the budget; 10) information concerning the proprietary obligations of the holder of information; 11) information on the property of the holder of information; 12) precepts which have entered into force and legislation which is issued by way of state supervision or supervisory control or under disciplinary procedure and information relating to punishments in force.'

Information on nuclear activities may also be regarded as exempt for the protection of national security. However, in cases of nuclear accidents, public interest of the affected population and other states to receive information, as well as the interest of mitigating the damage and further risks outweigh any potential to harm national security. Such obligation is regulated in the Convention on Early Notification of a Nuclear Accident and in the Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency.[233] The Chernobyl 'accident clearly demonstrated that the authorities have a duty to provide the public with clear and full information, but also that the public is entitled to this information. What is therefore needed is training for a large number of well-informed people who are familiar with information techniques to ensure that the public has a credible source of information. Furthermore, emergency plans should put the public in a position to assess their own risk of contamination'.[234]

2001 witnessed the enactment of the UNECE Convention on 'Access to Information, Public Participation in Decision-making, and Access to Justice in Environmental Matters' which now has 46 Parties and regulates this issue in Article 4 paragraph 4 as 'A request for environmental information may be refused if the disclosure would adversely affect: […] International relations, national defence or public security;', however in the same paragraph it also states that 'The aforementioned grounds for refusal shall be interpreted in a restrictive way, taking into account the public interest served by disclosure and taking into account whether the information requested relates to emissions into the environment'.[235] This means that the formula 'would adversely affect', has to be interpreted narrowly, and a public interest test also has to be performed.[236]

This is also found in state requirements. In the light of the Chernobyl accident, Article 50 of the Ukrainian Constitution stipulates that 'Everyone shall be guaranteed the right of free access to information about the environmental situation, the quality of foodstuffs and consumer goods, as well as the right to disseminate such information. No one shall make such information secret', while 'the Russian Federation Law on State Secrets declares that information, inter alia, on the state of the environment, health and sanitary data is excluded from being desgnated a State secret'.[237]

RECOMMENDATION

Lists of prohibitions on classification strengthen the right of access to information as well, since they support effective whistleblower legislations. Prohibitions should be designed on the basis of the (mal)practice of the public bodies, taking into consideration in which areas the highest risk of illegitimate classification for concealing wrongdoings is present.

9. Scope of the laws

Which bodies and which lifecycles of information are covered by freedom of information and classification laws?

The personal scope (concerning both natural and legal persons) of application of the freedom of information laws vary quite significantly from country to country. Differences are based on a number of variables such as federal structure of the country, specialised freedom of information provisions, laws of certain sectors, constitutional traditions, etc. Some countries exclude certain authorities from the application of their freedom of information acts. For example in the United States or Hungary there is no authority which would be exempt from the freedom of information act, while in the United Kingdom thirteen authorities in the field of national security, defence and law enforcement are.[238] In Australia among others, the Australian Government Solicitor, Australian Secret Intelligence Service, Australian Security Intelligence Organisation, Inspector-General of Intelligence and Security are also exempt.[239]

For example in Hungary the scope of the law 'encompasses all data control and data processing activities undertaken in Hungary'.[240] Whereas in the Czech Republic the law stipulates that

> '(1) The bodies obliged to provide information related to the scope of their powers under this Act shall be state authorities, territorial self-administration entities and their authorities, and public institutions. (2) Such obligated bodies shall also include the bodies that have been authorized by the law to decide entrusted by the law with making decisions on the rights, legislatively protected interests or duties of natural persons and legal entities in the public administration sector. Such duty applies solely to the scope of their discretionary powers'.[241]

Exemptions serve the protection of well-defined areas of public or private interests, such as defence, foreign relations, business secrecy, or privacy. A 'particular state, public authority or unit' itself is not a public interest to be served. Only their activities may be in the interest of the public. In some cases public interest is best satisfied by not disclosing information concerning these activities. For example in the German Federal Freedom of Information Act, the intelligence services are not fully exempted, only their covert activities: 'with regard to the intelligence services and the authorities and other public bodies of the Federal Government, where these perform duties pursuant to Section 10, no. 3 of the

Security Clearance Check Act (SÜG)'.[242]

It is an important aspect of these laws that, in those cases where exemptions apply to information related to the activities of entire agencies, a very significant means of accountability fall away and hardly any other legal solution can replace them. Therefore, it is recommended that a general freedom of information legislation covers all public bodies and no entity is exempt from it. Yet, certain pieces of information may be withheld in line with legal exemptions. **Principle 5** addresses the issue of exempting public bodies:

a. 'No public authority—including the judiciary, the legislature, oversight institutions, intelligence agencies, the armed forces, police, other security agencies, the offices of the head of state and government, and any component offices of the foregoing—may be exempted from disclosure requirements.

b. Information may not be withheld on national security grounds simply on the basis that it was generated by, or shared with, a foreign state or inter-governmental body, or a particular public authority or unit within an authority.

Note: Concerning information generated by a foreign state or inter-governmental body, see Principle 9(a)(v)'.

PRINCIPLE 13

a. Only officials specifically authorized or designated, as defined by law, may classify information. If an undesignated official believes that information should be classified, the information may be deemed classified for a brief and expressly defined period of time until a designated official has reviewed the recommendation for classification.
Note: In the absence of legal provisions controlling the authority to classify, it is good practice to at least specify such delegation authority in a regulation.

b. The identity of the person responsible for a classification decision should be traceable or indicated on the document, unless compelling reasons exist to withhold the identity, so as to ensure accountability.

c. Those officials designated by law should assign original classification authority to the smallest number of senior subordinates that is administratively efficient.
Note: It is a good practice to publish information about the number of people who have authority to classify, and the number of people who have access to classified information.

10. Authority to classify

Who decides on whether a piece of information needs a heightened level of protection and if the right of access to such information should be restricted?

Any restriction on right of access to information has to be prescribed by law (see Chapter 3.2). This authority shall be exercised by public officials whose power can clearly be traced back to acts of Parliament, and even if indirectly, are responsible to Parliament. In the Swedish system, 'the Government may not decide on which documents are secret; this is an exclusive right of the Riksdag [Parliament]. However, in a number of provisions of Public Access to Information and Secrecy Act, the Government is empowered to make supplementary regulations'.[243]

The authority of restriction consists of various competences regarding classified information, such as use for official purposes, processing, registering, holding, classifying, marking and re-marking, copying, translating, extracting content, transferring, referring, disposing, authorising access, authorising use, reviewing and declassifying. Generally the classification, which is the strongest competence, is anchored in law and the person who is authorised to classify information is allowed to exercise other competences. Delegation of competences may be limited by law.

The above mentioned competences are distributed according to the hierarchy of the government, judiciary, and legislative branches of power. Though every government has a different 'anatomy' and different arrangement of powers and responsibilities for which classified information is needed, there remain certain principles which are common in the classification regimes.

There are three important principles present in all examined secrecy regimes.[244] First, anybody who has any access to classified information must be vetted so as to provide *personnel security* to the protected information. The rules of security vetting are often included in the secrecy laws – however this issue is out of the scope of this study. Second, access to classified information can be provided exclusively to those, regardless of their position in administrative hierarchy, who need the specific information for official purposes – this is the principle of *need to know*. Third, the originator of (the organ which created/classified) the classified information has ultimate control over the distribution of the information. Moreover the information cannot be declassified by other organs or without the consent of the originator – this is the principle of *originator control* (see chapter 6).[245]

In Slovenia and Macedonia (FYR) only the highest dignitaries such as the President of the (National) Assembly, President of the Republic, ministers (in Macedonia (FYR) *within their sphere of activity)*, etc. and persons authorised by them can classify information as top secret.[246] The same group of positions in Austria, Czech Republic, Estonia, Hungary, Lithuania, Poland and Slovenia '*may have* access' to information *without* demonstrating a justified need to know. Although there are no provisions that these privileges cannot be delegated, it is obvious based on the nature of the authority. Furthermore there may be exceptions based on international obligations.

In many countries, in addition to the usual list of the Executive, the Legislative and the Judiciary organs, the National Bank, the contractors in defence and national security matters, a wide range of other organs (and their heads) are enlisted as having full or partial classification authority: State Audit Office[247], Ombudsman[248], Competition Authority, Academy of Sciences and even the Administration of National Pension Insurance[249]. The standards of the Republic of South Africa offer an even wider scope: 'All bodies/institutions/organisations have at their disposal intelligence/information that is to some extent sensitive in nature and obviously requires security measures'.[250]

The delegation of classification authority within the public bodies is an additional question. There are some rules of thumb which help to keep the line of authority delegation clear. The delegation should be in written form, so that the line of authority can be traced back to the head of the public body.[251] It is a further rule, implicit in the functioning of any administration and explicit in the Republic of South Africa, that *'Delegatus delegare non potest* - A delegate cannot delegate'.[252] In New Zealand, 'Chief Executives and heads may delegate authority to classify to senior staff, but sparingly. In particular, only appropriate senior staff should be given authority to classify material SECRET or TOP SECRET. It is important to avoid unwarranted application of these classifications by less experienced staff'.[253]

The classification system of the United States specifies both original and derivative classification authorities. 'Original classification is the initial determination that information requires protection. Only U.S. Government officials to whom this authority has been delegated in writing, and who have been trained in classification requirements, have the authority for original classification. Original classification authorities issue security classification guides that others use in making derivative classification decisions. Most government employees and contractors make derivative classification decisions. In 2011 there were 2362 government employees who had Original Classification Authority.[254]

Derivative classification is the act of classifying a specific item of information or material, on the basis of an original classification decision already made by an authorized original classification authority. The source of authority for derivative classification ordinarily consists of a previously classified document or a classification guide issued by an original classification authority'.[255]

As described in the above quote not only the proper authorisation, but also the adequate professional knowledge of the originator, is crucial in operating a functional classification regime. In Poland, the law prescribes the training of public officials as 'the organisation heads shall arrange for their employees to be trained in ranking

classified information, in giving appropriate secrecy classifications in the secrecy classification modification and removal procedures'.[256] The UK Security Policy reminds that

> 'Fostering a professional culture and developing a positive attitude toward security is critical to the successful delivery of this framework. Security must be seen as an integral part of and a key enabler to, effective departmental business. Departments and Agencies must ensure that all staff are briefed on their security responsibilities on induction and have access to regular refresher training, awareness programmes and security briefings. These should cover individual responsibilities, as defined by the Civil Service Code, including the reporting of security incidents and criminal behaviour and / or any knowledge of leaking. In addition to line management reporting, all staff must also have recourse to consult with, or report anonymously to counselling and support services or to an independent arbiter'.[257]

New Zealand rules also require training, mainly on security risks.[258] Obviously, other systems also train public officials handling classified information, even if it is less emphasized in legal texts.

RECOMMENDATION

Information on how information is classified should never itself be considered classified since it is a prerequisite of the verification of the validity of classification.

Training of public officials originating or handling classified information should include education on freedom of information.

Keep track of number of people with authorisation to classify information and make this information public.

11. Reviews and Declassification

Information may be classified and withheld from public domain, but not forever. What are the procedures and conditions for removing classification?

It is a basic concept of record management that records (information) have life-cycle. '[B]oth classified and unclassified information (and the records in which that information is contained) exists throughout a life span in which decisions must be made with respect to creation, management and use, and final status (typically either destruction or preservation and release)'.[259] Throughout, lifecycle consideration has to be given to whether the information needs to be protected as classified and, if so, whether the classification should be upheld in its original form. As the importance of information is changing over time (disclosure that can cause serious harm today may be totally irrelevant within a year), the necessity of measures to withhold information from the public has to be reviewed from time to time. This is so that nobody's fundamental right to know should be restricted any longer than needed, in line with the above detailed principles (Chapter 3). Reviews have an essential role in preserving the sound functioning of the classification system, whose implications extend far beyond the very significant costs of information security. As US Supreme Court Justice Potter Stewart pointed out in the Pentagon Papers case

> 'when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion. I should suppose, in short, that the hallmark of a truly effective internal security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained'.[260]

For these reasons, every secrecy regime has some internal review mechanism. Basically there could be four kinds of review: *regular reviews* embracing all information classified within a certain period; *random checks* [261] that primarily serve the security of the classified information; review *on initiative of the public body* (for example in the case of a major scandal); and *review on request.*[262]

The Australian guidelines warn '[a]s protective markings make information more expensive to handle, store and transfer, agencies are encouraged to have a procedure for confirming initial markings, especially where the protective marking is not normal or standard for that agency'.[263] The Security Policy of the United Kingdom, used not only to give details on the review mechanisms, but also highlighted the importance of reviews, as sometimes 'the protective marking may no longer be current, and, while it reflects the highest classification of the information contained in a document, the file may also contain information that is not sensitive and may be subject to disclosure in a redacted form'.[264]

A review may have different outcomes: 1) the classification level and the period of classification is maintained; 2) the classification level is downgraded and the period is reduced; 3) the information is reclassified at a higher level and/or the period is extended; 4) the information is declassified.

The principle of originator control also applies to reviews of classified information. Thus, all public bodies holding copies of the information should be notified on the outcome of the review performed by the originator.[265] Therefore if either an internal or an external review results in change of classification, all entities that hold the classified information have to handle it in line with the reviewed information/ document's new classification.

PRINCIPLE 17

a. National legislation should identify government responsibility to coordinate, oversee, and implement government declassification activities, including consolidating and regularly updating declassification guidance.

b. Procedures should be put in place to identify classified information of public interest for priority declassification. If information of public interest, including information that falls into categories listed in Principle 10, is classified due to exceptional sensitivity, it should be declassified as rapidly as possible.

c. National legislation should establish procedures for en bloc (bulk and/or sampling) declassification.

d. National legislation should identify fixed periods for automatic declassification for different categories of classified information. To minimize the burden of declassification, records should be automatically declassified without review wherever possible.

e. National legislation should set out an accessible and public procedure for requesting declassification of documents.

f. Declassified documents, including those declassified by courts, tribunals or other oversight, ombuds, or appeal bodies, should be proactively disclosed or otherwise made publicly accessible (for instance, through harmonization with legislation on national archives or access to information or both).
Note: This Principle is without prejudice to the proviso regarding other grounds for withholding set forth in preambular paragraph 15.

Note: Additional good practices include the following:

- *regular consideration of the use of new technologies in the processes of declassification; and*
- *regular consultation with people with professional expertise concerning the process for establishing declassification priorities, including both automatic and en bloc declassification.*

11.1 INTERNAL REVIEW OF CLASSIFICATION PROCEDURE

The period of reviews, if there is any prescribed by law, varies in different countries. According to the former law of Estonia, the classified media has to be reviewed at 'least once a year and, upon expiry of classification'.[266] In the Czech Republic and Hungary the classification has to be 'reviewed no less frequently than every five years from the date of its creation'.[267] Similarly, EU classified information has to be reviewed 'no less frequently than every 5 years. Such a review shall not be necessary where the originator has indicated from the outset that the information will automatically be downgraded or declassified and the information has been marked accordingly'.[268] In Macedonia (FYR), top secret classification has to be reviewed in a period no longer than ten years, secret classification – five years, confidential classification – three years, and restricted classification – two years.[269]

There are additional rules regulating when reviews should be performed. The German regulation prescribes that a review of classification should be performed before the information is provided to a private individual or company.[270] The New Zealand manual gives practical details on downgrading:

- 'automatically downgrade information that becomes generally known after an event such as operations, moves, conferences, constitutional changes or visits
- review accumulated material for downgrade, or destroy surplus material that is not required for records, after an operation or sequence of events
- review files, media and contents for regrading when they are taken out of or brought back into current use
- review accountable documents for regrading when they are mustered for periodical checks
- review technical or scientific reports for regrading when they are over five years old, or some other specified period'.[271]

The Estonian law has a provision related to *premature declassification of information classified as state secret* which takes into consideration information of public interest (see Chapter 8). As a rule, information concerning undercover agents, police agents, and other officials in similar positions is classified as state secret and remains classified during the lifetime of the person concerned, unless the concerned person provides written consent and specifies the extent of disclosure.

PRINCIPLE 14

Public personnel, including those affiliated with the security sector, who believe that information has been improperly classified may challenge the classification of the information.

Note: Security sector personnel are flagged as deserving of special encouragement to challenge classification given the heightened cultures of secrecy in security agencies, the fact that most countries have not established or designated an independent body to receive complaints from security personnel, and disclosure of security information often results in higher penalties than does disclosure of other information.

However there is an exception: 'if the person has been convicted of intentionally committed criminal offence against the state or a crime against humanity', which means such information can be declassified already during his/her lifetime without his/her consent.[272]

Even if there are regular reviews, this by itself is not sufficient to halt over-classification. Therefore if the review results in extension of the classification period, additional controls would be needed to ensure against wanton classification.

In Estonia, the former secrecy act prescribed that 'an application for extension of the term of classification of information which is classified as a state secret shall be submitted to the [head of the originating body] as appropriate at least three months before expiry of the term of classification of the information'.

This means the originator has to review the classification in time and cannot opt for withholding information at the last minute, because he/she may believe there is no time for a proper review and it is safer not to disclose anything by extending the expiry of classification.[273] In Lithuania, the Commission for Secrets Protection Co-ordination can decide on extension.[274] The possibility of extension is limited to exceptional cases in Mexico.[275]

The Polish and Slovene acts, as well as the Australian guidelines, contain controls on improper or over-classification. Both the present and the former Polish law stipulate that 'in the event that a certain material has been given an evidently overrated or underrated secrecy classification, the recipient of the same shall notify the person referred to in clause 1 or that person's superior'.[276] However, provisions of neither laws are 'stipulating the type of responsibility that a state official might face for excessive classification'[277] as Piotr Niemczyk points out

> 'The superior is unable to control all classified information generated within the organizational unit and thus is unable to supervise the conduct of all officials. Therefore, it is possible that people, in order to hide their own incompetence, or that of other officials, choose to classify information even where, it is not obligatory. Under PCIA 1999, which also did not provide for sanctions, in practice, officials rarely faced responsibility for misconduct through disciplinary measures. Therefore, it is fair to assume that PCIA 2010 will not provide a significant change in holding officials responsible for their abuses concerning misclassification. Although the procedure exists, it will be difficult to enorce it'.[278]

In Slovenia, 'users that have legally received classified information may propose to the authorised person that a particular classification that they deem unjustified or incorrect be changed. The authorised person shall consider the proposal from the preceding paragraph and notify the proposer of the decision taken'.[279] In Australia, 'all recipients of information are encouraged to contact the originator to discuss any security classification they believe is inaccurate'.[280]

RECOMMENDATION

Regular reviews of all information should be performed no less frequently than every five years of its creation. Reviews should be performed in any case of request of classified information too.

Information management systems should be in place, which provide up to date information on any classified information, with regard to basic information on classification and justification. Information management systems should be able to provide statistics and basis for detailed evaluation of the classification and review system. The same systems should be able to serve as a basis of registers.

Detailed statistics should be collected and published on the results of the reviews.

11.2 EXTERNAL REVIEW OF CLASSIFICATION PROCEDURE

The examined secrecy laws do not discuss the external review procedures. Specific provisions on the external review of classification in the FOI Acts are scarce as well. The FOI laws provide for review mechanisms related to access to information. Yet classification systems are separately regulated and in most cases FOI leave these laws and regulations untouched (see Chapter 3.1). However, the general rule in the field of classification is that it is up to the administrative system which decisions of which bodies can be overruled by its superior entities or oversight authorities. This rule applied to secrecy regimes means that the originator controls the classification. Thus if the head of the public body is declared as originator by law (see Chapter 10) then he/she will have the final word within the public body. If there is any supervisory body of the originator, that body may call for changing the classification or declassify that piece of information and not call for it. Nonetheless, the originator – which is usually a specialised body with the necessary knowledge of the classified information and all of the relevant details of classification – has to perform the review and the change/removal of classification.

No secrecy law among the ones examined contained provisions on court reviews. The Hungarian, Slovenian and Mexican FOI Acts have provisions on special procedures of reviews by the Information Commission(er) (see below) in which courts also have a role. Furthermore, the general FOI rules of court procedures apply in case request of disclosure of (classified) information is denied. If the court orders disclosure of classified information the situation is similar to when the supervisory body orders disclosure: in these countries only the originator can remove classification and whether the originator complies with the decision of the court or of the supervisory body is a question of execution. Nevertheless, it is conceivable that to regulate this issue the court is given the authority to remove classification. However, the courts often tend to defer such acts to the Executive.

The matter of declassification of information and practical access to declassified information reached the level of international courts, when in the case of *Kenedi v. Hungary* the ECtHR found violation of Articles 6, 10 and 13 of the ECHR. In this case the applicant was unable to gain access to declassified and later reclassified documents, despite the court had ordered disclosure of the information.

> 'The Court observes that the applicant obtained a court judgment granting him access to the documents in question (see paragraph 10 above). Thereafter, a dispute evolved as to the extent of that access. However, the Court notes that, in line with the original decision, the domestic courts repeatedly found for the applicant in the ensuing proceedings for enforcement and fined the respondent Ministry. In these circumstances, the Court cannot but conclude that the obstinate reluctance of the respondent State's authorities to comply with the execution orders was in defiance of domestic law and tantamount to arbitrariness. The essentially obstructive character of this behaviour is also manifest in that it led to the finding of a violation of Article 6 § 1 of the Convention (see paragraph 39 above) from the perspective of the length of the proceedings. For the Court, such a misuse of the power vested in the authorities cannot be characterised as a measure "prescribed by law"'.[281]

In several countries, various entities of the Executive have to provide for access to information which were improperly or unlawfully classified or failed to be unclassified. For instance, the Estonian Committee for the Protection of State Secrets has the duty to 'review petitions and complaints concerning the unlawful application of or failure to apply this [secrecy] Act or legislation issued on the basis thereof (...) and shall inform the Government of the Republic of the results of the review'.[282] In Germany, the Federal Archives have the right to ask for the review of the seemingly unjustified or overly long classification of information held by them.[283] In the Czech Republic, the Control Body, established by the Chamber of Deputies, has the right to examine the activity of the National Security Authority whether it 'unlawfully restricts or infringes on the rights and liberties of citizens' and also 'entitled to ask for a necessary explanation from the director of the Authority'.[284]

The first prerequisite that the Commission(er) can properly review any classification is their authority to access any classified information. The Hungarian[285], Mexican and Slovenian Information Commission(ers), as well as for example the Czech Ombudsman and Deputy Ombudsman[286], the European Ombudsman[287], the Ombudsmen of New Zealand[288] and the Public Protector of the Republic of South Africa[289] have this power. The second prerequisite is that the Commission(ers) themselves have the authority to remove classification, to order the removal of classification or to initiate a court procedure for declassification.

Compared to the commissioners, the powers of the ombudsmen are rather limited as they can issue recommendations, but cannot enforce the recommendation - their power lies in their publicity. The powers of the Information Commissioners are more effective in achieving the disclosure of information if it was withheld illegally or the classification was unjustified.

However, both systems lead to the same outcome: the courts will have the final decision in these matters. In the first case, as the recommendations have no legal binding power, therefore if the requestor is unsatisfied with the outcome of the ombudsman investigation or with the response of the public body, then only a court procedure may result in enforceable order to disclose information. In the second case, if the Information Commission(er) has the authority to order disclosure, it still needs an appeal mechanism as in a rule of law system all administrative decisions have to be subject to possible remedies. In this case, a binding decision of the Information Commission(er) is to be considered as an administrative decision.

The strongest authority in this field is provided to the Mexican Commission: 'At any moment, the Institute may have access to classified or confidential information in order to determine the category to which the information belongs, whether it is properly classified, declassified or the procedure by which access should be granted'.[290]

According to the Hungarian law, if the National Authority for Data Protection and Freedom of Information, before 2012 the Information Commissioner (hereinafter: the Authority), finds that the law on protection of classified information has been violated, the Authority instructs the classifier to modify the classification level and its period of validity in compliance with relevant legislation or alternatively to terminate classification. 'Should the classifier deem that the decision made by the Authority, in accordance with subsection (1), is unfounded, the classifier may request that it be reviewed by a court within a period of 60 days of the announcement of the decision. The execution of the decision can be delayed by submitting a statement of claim. Should the classifier not turn to the courts within a 60-day period beginning on the date the decision was announced, the classification of the national classified information becomes null and void. On the 61st day following the announcement of the decision, its classification level or period of validity changes in accordance with the decision'.[291] The Court shall conduct its proceedings in-camera and out of turn. In its decision it may affirm, change or invalidate the decision of the Authority or order the Authority to conduct a new procedure.

In Slovenia, '[i]f the applicant holds, that information is denoted classified in violation of the Act governing classified data, he can request the withdrawal of the classification' and the Commissioner shall decide on the appeal.[292] The law also provides for that 'administrative dispute may begin against the decision by the Commissioner in accordance with the statute'.[293]

In the common law countries where public bodies have the authority to issue certificates in national security matters, the authority of the Commissioner or Ombudsman is more limited and such certificates can be appealed before courts (see Chapter 7.3).

11.3 ILLEGAL DISCLOSURES

Do illegal disclosure of information and its entry into the public domain void the classification?

None of the examined secrecy laws in force contain provisions on whether illegal disclosure renders void the classification. Usually, there are provisions that if anybody finds classified information anywhere it should be returned to the originator. Yet there are few provisions about what happens if classified information is disclosed without authorisation to a few people or to the wider public, i.e. on mass to media/ newspapers or on the Internet.[294]

In Slovenia, 'during the first reading phase, the proposal for this act contained a provision that "the confidentiality of information does not terminate if it is disclosed to an unauthorised public, or if an identical or similar information is disclosed" (Part 2, Art. 7 of the proposal of the Classified Information Act, first reading Porocevalec DZ, No. 10/00 of 18.2.2000, p. 134)'.[295] In Estonia, the former secrecy act contained a provision that 'the classification of a medium shall not expire by reason that information contained therein has been unlawfully disclosed or information similar to the state secret contained in the classified medium has been disclosed', by contrast the new act remains silent on this matter.[296] The New Zealand manual does not mention illegality when it recommends that public bodies should 'automatically downgrade information that becomes generally known after an event such as operations, moves, conferences, constitutional changes or visits'.[297]

It is noticeable that countries that regulate that classification is not invalidated by disclosure may not be in line with the practice of the ECtHR. In the case of Weekblad Bluf! vs. The Netherlands, the court pointed out 'that it has already held that it was unnecessary to prevent the disclosure of certain information seeing that it had already been made public or had ceased to be confidential'. Moreover, even if in this case the report could not be obtained by other means and the Netherlands authorities had brought proceedings to prevent publication, as 'the information in question was made accessible to a large number of people, who were able in their turn to communicate it to others. Furthermore, the events were commented on by the media. That being so, the protection of the information as a state secret was no longer justified and the withdrawal of issue no. 267 of Bluf! no longer appeared necessary to achieve the legitimate aim pursued'.[298]

The EU prescribes that if 'there are reasonable grounds to assume that EUCI has been compromised or lost, the competent security authority shall take all appropriate measures in accordance with the relevant laws and regulations to: (a) inform the originator; (b) ensure that the case is investigated by personnel not immediately concerned with the breach in order to establish the facts; (c) assess the potential damage caused to the interests of the EU or of the Member States; (d) take appropriate measures to prevent a recurrence; and (e) notify the appropriate authorities of the action taken', but it doesn't regulate the issue of validity of classification.[299]

RECOMMENDATION

There should be explicit rules on the legal consequences regarding the status of information which was marked as classified but enters into the public domain by illegal disclosure. In the public domain classification should be void.

11.4 DECLASSIFICATION

Secrecy laws rarely discuss the issue of what happens after a document or information is declassified. Yet there are some provisions dealing with this issue in the laws of the studied countries. When the Hungarian Constitutional Court abolished the entire classification system of the former non-democratic regime, it reasoned that

> '[t]he open, transparent and controllable activity of public authority, and the public operation of State authorities and the executive power in general constitute a cornerstone of democracy and a guarantee of the rule of law. Without the test of publicity, the State becomes 'a machine alienated' from its citizens, and its operation becomes incalculable, unpredictable and expressly dangerous, because the lack of transparency of the State's operation poses a great danger to the constitutional freedoms'.[300]

Sound declassification rules can protect societies from such risks. Declassification is the momentum which provides evidence of the legality and reasonableness of classification – declassification is the public's test.

Declassification can be the result of a review, expiry of time (Chapter 12) and in some cases of illegal disclosure.

If information is declassified due to expiry of time or a review, protection of classified information laws occasionally regulate the next step in their life-cycle, though sometimes these regulations remain silent and such provisions may be found in laws on archives.

In Lithuanian law, practical terms can be found when it prescribes 'detailed lists of declassified information shall be approved and modified by managers of subjects of secrets co-ordinating of the lists with the Commission for Secrets Protection Co-ordination of the Republic of Lithuania'.[301] The New Zealand manual is more progressive and refers to the Archives Act and details the procedure in which the public body declassifying information has to cooperate with archivists and as a main rule declassified information will be accessible.[302] According to German regulation, the documentation on declassification, lists of material transferred to the National Archives, and the declassifying decision all have to be published on the www.bundesarchiv.de website of the National Archives.[303] Under Mexican law, '[r]equests for access to information and responses to them, including the information delivered in such cases, will be public. Likewise, the agencies and entities must place this information at the public's disposition, when possible by remote or local electronic means', which means if information was declassified on request it will be available online.[304]

This study cannot discuss the crossing points between archival laws and freedom of information. There is very extensive literature on archives, national security archives and military archives. Numerous international organisations are active in this field such as the UNESCO[305] and the Council of Europe[306].

RECOMMENDATION

Detailed lists containing basic information on declassified information should be proactively published.

11.5 EVALUATION OF (DE)CLASSIFICATION PRACTICE

There are several entities that can or could evaluate classification practice in a country: information commission(er)s, National Security Authorities (hereinafter: NSAs), special commissions, Parliamentary committees, etc. However, even if in a country there is a specialised body of freedom of information, such as an information commission(er) it does not necessarily mean that it supervises or evaluates compliance of government agencies with the classification rules as very often they are not entrusted by law to do so.

By contrast, the main role of NSAs, established following NATO and EU security rules both in member states and in other countries cooperating with NATO or EU, is to protect classified information. In theory they could also examine freedom of information issues in the context of protection of classified information. Nonetheless, based on the approach of the NATO and EU security standards, access to information is merely a secondary question, thus not much can be learned from these bodies from a freedom of information point of view.

Regardless of how reluctant National Security Authorities may be, access to information falls within the ambit of NATO and EU security rules and consequently within their competence. Furthermore, as NSAs have an active role in enforcing the secrecy laws they (could) have an important role concerning the exercise of the right of access to information.

NSAs are entrusted with maintaining a functional secrecy regime in the entire public administration and also in the field of industrial security or international co-operations in which classified information is used. Secrecy and other stand-alone laws prescribe the powers and obligations of the NSAs. Though the list of duties varies, the baseline of their content is set by the EU and the NATO. In the EU and for NATO member states, the role of evaluating the practice of secrecy regimes is delegated to NSAs. Information commission(er)s may issue recommendations on freedom of information issues. The NSAs have access to classified information in the public administration and due to their responsibilities they have oversight over entire classification systems. At the same time NSAs' attitudes are defined by security risks and needs, while the values of freedom of information are hardly internalised by these bodies. As a consequence, feedbacks based on their experience may rarely be confronted or reconciled with the right of access to information. Further, their proposals on policy decisions concerning secrecy legislations may be limited to information security aspects.

As NSAs have eminent roles in classification systems, it may be worth assessing their stance towards openness as rules governing their functioning are unlikely to contain provisions on freedom of information. It can be seen as a sign of the openness or secretiveness of the work of NSAs whether they have a website and if any information is published on their findings of the national secrecy regime.

Among the examined sixteen regimes, at least fourteen have NSAs or other public bodies fulfilling this role (we could not identify the Mexican and the South African). Half of them have their own websites. In the case of Australia, Austria, the European Council, Germany, Sweden and the United Kingdom either other official websites referred to their existence or we presume they exist due to these countries' international obligations. Among those NSAs which have websites only three published any of their annual reports in English: the Czech Republic, New Zealand and Poland.[307]

None of them contains statistics on the classification and declassification practice and a significant part of the New Zealand report is classified. That being said, the Czech and the Polish reports give detailed insight to the most common problems of classification, without compromising the national security of these countries. Unfortunately, in the examined countries no reports were found which would be as detailed and informative as those prepared by the Information Security Oversight Office (ISOO) responsible to the President of the United States or by the Public Interest Declassification Board (PIDB) which is an advisory committee established by Congress of the United States.[308] Another good example of openness in this field is Bulgaria where '[t]he State Commission on Information Security (SCIS) held public discussions in 2010 and 2011 in order to assess the need to issue binding instructions with regard to this classification' so as 'to define what information shall be classified as official secret'. In 2012 the same national security authority also organised trainings with participation of the civil society organisation Access to Information Programe.[309]

RECOMMENDATION

NSAs should prepare detailed reports on the practice of classification and declassification and should publish these reports at least in the official language of the country and preferably in foreign languages if the use of another language is required due to their memberships in international bodies.

Reporting systems should be established/enhanced to enable the NSAs to assess whether the classification practice complies not only with security requirements, but also FOI provisions.

Reports should comprise both statistical data and analysis of classification and declassification practice. The work of the ISOO and PIDB in the United States may set a good example in this area.

NSAs should regularly hold public consultation to review categories of classification of information.

The General Secretariat of the Council of the European Union and the NATO Office of Security should encourage the development of common standards of reporting, statistical methodology and terms of reference for analysis. Expertise of archivists, information management professionals and members of truth commissions may be used in this work as well.

12. Expiry of classification and overlapping secrets

For how long does a secret need protection by classification? Is there a maximum? Which secrets need longer protection periods?

Classification is a restriction of the right of access to information. In a rule of law system, no restriction can be unlimited in any sense without voiding the right. With the passage of time, and as the sensitivties regarding information reduce, there is a need to limit how long information can be classified for.

12.1 TIME LIMITS FOR PERIOD OF CLASSIFICATION

Classification periods vary quite significantly. The shortest is in Mexico where 12 years is the maximum which can be extended only in exceptional cases[310]. In the United States the default is 10 years and initially information cannot be classified for a period longer than 25 years.[311] The Australian rules follow the US, the default is 10 years and the maximum is defined by the Archives Act.[312] It is difficult to determine what is the longest period of classification, as in Lithuania the classification period of state secrets can be extended by 10 years as many times as needed.[313] Similarly, in Poland, 'the new law introducing non-automatic declassification based on periodic revision did not exclude from the Polish legal scheme a permanent classification of certain sensitive data, namely identification data concerning officers, soldiers, or other persons participating in operational activities'.[314] After discounting the indefinite and endless limitation periods, Hungary has the highest time limit: the maximum is 30 years and further extensions of 30+30 years 'with regard to defence, national security, criminal prosecution or judiciary interests if it is closely related to a lawful interest of a private person'.

Moreover, in Estonia the maximum is 75 years for among others 'items of information concerning the persons and undercover agents recruited for secret co-operation by surveillance agencies'[315] and in Sweden the maximum is 70 years.[316] In the middle there is Germany with 30 years which can be extended to 60 years.[317]

It is a further characteristic of these legislations that there are some exceptions as regards the maximum period. In Poland the new law abolished

> 'the time limit after which data is automatically declassified. Instead, PCIA 2010 provided for the obligatory review of information not less that

PRINCIPLE 16

a. Information may be withheld on national security grounds for only as long as necessary to protect a legitimate national security interest. Decisions to withhold information should be reviewed periodically in order to ensure that this Principle is met.
Note: It is good practice for review to be required by statute at least every five years. Several countries require review after shorter periods.

b. The classifier should specify the date, conditions, or event on which the classification shall lapse.
Note: It is good practice that this time limit, or specification of conditions or event on which classification lapses, is subjected to periodic review.

c. No information may remain classified indefinitely. The presumptive maximum period of classification on national security grounds should be established by law.

every five years to check whether the information continues to fulfil the prerequisites to be protected under the classification regime. PCIA 2010 also grants a classifier the competence to identify a date or specific event for declassification or alteration of classification level. The shift abandons a strict time limit and introduces a more flexible system of declassification that is, however, based on the discretion of declassification authority'.[318]

At the same time, a provision of the old law lives on in the new one and the following information shall be subject to protection regardless of the elapse of time:

1. 'data identifying the civilian and military state security services staff engaged in operational-surveillance tasks;

2. data identifying those who assisted the state bodies, services and institutions authorised under this Act to carry out operational-surveillance tasks in the execution thereof; (and)

3. that classified information obtained from other states or international organisations which has been supplied subject to that condition'.[319]

Information falling under the first two categories of the cited Polish provision is commonly protected for a longer period or even indefinitely. Information pertaining to the third category never has an expiry attached to according to national rules. There is one more category which is commonly exempted from maximum expiry time: details of infrastructure for military of national security purposes, such as plans of buildings, rooms, constructions, security and communications systems, etc.

RECOMMENDATION

Freedom of information is a human right and no human right shall be restricted for an indefinite time period. There should be maximum expiry time in every secrecy regime.

Between 12 and 95 years, the difference is considerable. The maximum period should be 20 years with exception to military / national security infrastructure and staff and collaborators.

Extensions should require the approval of the supervisory authority.

Secrecy rules should make it clear that by expiry of time, without any further formal action, classification cease to exist.

Such information remains classified as long as these buildings are possessed by or serve national security or defence bodies.[320]

A question seemingly only of legal relevance raises a rather practical question of classification. Depending on the administrative legal system of the country, the declassification by expiration of time may occur in two ways. Either the public body holding the classified information has to declare formally that by expiry the classification ceased to exist; or without formal declaration by expiry the classification ceases to exist. Unfortunately the legal regulations analysed provide no certain answer in which country which interpretation is valid, though the required, but lacking formal declaration may pose a significant burden to individuals seeking access to information that was previously classified.

The existence of a maximum time period of expiry is a significant matter for the exercise of right of access to information. The Czech, EU, Macedonian, Slovenian, and UK rules do not set a maximum expiry time. They only require that a expiry time should be set and regular reviews should be performed. The New Zealand rules require 'transfers to the National Archives all 'public archives'—public records, with certain exceptions, at least 25 years old, no longer in use, and worthy of permanent preservation'.[321] For those regimes where there is a maximum expiry time, extension is a crucial question as an extension decision may double the length of time during which information is inaccessible to the public. The German, Lithuanian, Mexican and U.S. rules require the approval of higher level authorities (or of the Information Commission) if in exceptional cases the expiry time may be extended.[322]

12.2 AUTOMATIC DECLASSIFICATION

Automatic declassification is an uncommon but rather important feature of classification regimes. When the Legislation enacts rules of automatic declassification, it aims to make the Executive perform its declassification duty more intensely than it has performed previously. The reason for the adoption of such rules is the overload of the administration with classified information which has lost its sensitivity or never should have been classified at all. Automatic declassification rules provide a deadline for the classifying bodies to review the classification of certain categories or age of information. When the deadline expires the classification of those records which were not reviewed and extended cease to exist without any further action needed solely due to the operation of law.

It is a common legacy of all countries that went through a transition from dictatorship to democracy that the secrecy regimes of the dictatorships had to be replaced and the new democratic bodies had to take over the classified information created by the entities of the secret services, political police, etc. of the former system(s). These transitions often cut through the expiry time – if any was defined by the non-democratic regimes – and for example the laws of the post-socialist Czech Republic, Hungary [323] and Slovenia introduced provisions on automatic declassification after a transitional period, if the information is not being reclassified according the new laws.

However, automatic declassification does not necessarily require such profound political changes. Classified information can run rampant in stable democracies as well since they may require these measures. In the United States automatic declassification provisions have been codified for decades.[324] The current provisions go back to 1995 when the following rule was foreseen: 'within 5 years from the date of this order, all classified information contained in records that (1) are more than 25 years old […]shall be automatically declassified whether or not the records have been reviewed'. [325] This deadline has been extended several times and still faces serious challenges[326], but its importance is beyond doubt.

12.3 OVERLAPPING SECRETS

Classification, which can apply to any piece of information, is only the outermost shell of restrictions on access. For instance, in the case of a new weapon, even the information of its existence may be classified as secret, but when it is publicly known and demonstrated, the classification is lifted. Yet the new technical solutions may still constitute trade secrets of the manufacturer. Similarly, if the phone conversation of a crime suspect is wiretapped this fact may be considered a secret until it is used as evidence in a court. However, the suspects preserve their right to privacy and thus information for example on their illnesses or personal life shall not be disclosed to anyone, unless it constitutes an integral part of the evidence and inevitably is needed to prove or dismiss the charges. Another

example was detailed above: information concerning security services staff engaged in operation is protected not only in the interest of national security, but also to safeguard other interest such as the personal safety of the security services staff as well as their privacy.

The Australian guidelines explain that 'each exemption stands alone and must not be interpreted as limited in its scope or operation by the provisions of any other exemption. Each exemption should be given its full meaning and no implications should be drawn from the terms of the other exemptions'. It also adds 'decision makers need to keep in mind the possible availability of other exemptions. However, only significant and supportable claims should be made'.[327] This logic is present in any freedom of information regime, but some of them have specific provisions regulating the question of overlapping secrets. In Mexico, personal data is considered as confidential information and the law emphasises that confidential information has no expiry unlike classified (reserved) information.[328] The Polish law stipulates that 'this act shall be without prejudice to the provisions on the protection of trade secrets or other legally protected secrets laid down in other Acts'.[329] The explanatory notes on the commentary of the German regulation warn that even if the information is declassified the common confidentiality rules still apply.[330]

It is noteworthy that only pieces of information may be classified or withheld under an (or several) exemption(s), but entire documents shall not be classified as they can contain different types of information falling under various exemptions. In the first case, when information is classified, different exemptions regarding the same piece of information have to be examined. In the second case, when documents are classified, every single piece of information needs examination, contained therein. However, in the latter case partial disclosure may be possible.

RECOMMENDATION

Every legal system sets up adequate measures to protect information which falls under an exemption of the FOI law. No information should be classified for reasons other than those allowed by classification rules. Classification regimes should be maintained only for protection of public interest as regulated by laws. The use of classification system for the protection of any other interest which falls outside of the scope of the classification law should be considered as abuse of the law.

For example, if the rules only allow for classification on the grounds of national security, defence and foreign relations, business secret should not be protected as classified information.

13. Access to information by oversight bodies

Do oversight bodies have access to everything?

There is a wide variety of independent oversight bodies which monitor or control the functioning of government agencies. Ombudsmen, parliamentary commissioners, and various appeal bodies belong to this category and all of them need access to information within their remit to enable them to exercise their authority on a substantive level.

Oversight of the implementation of freedom of information and secrecy laws has to be distinguished from the oversight of defence and national security entities. The latter category is not covered by this study, but the oversight of intelligence and security services is discussed in details by a recent study of the Geneva Centre for the Democratic Control of Armed Forces (DCAF).[331]

Oversight bodies that provide for the implementation of freedom of information and secrecy laws have very different roles. Some can initiate inspections performed by other authorities; others have the authority and capacity to perform inspection on their own. If violations of legal or internal rules are found, there are bodies which can issue only recommendations or statements (ombudspersons). Other entities may order review or review themselves decisions regarding access to information, classification, etc. Regardless of the exact scope of authority of an oversight/ ombudsperson/appeal body, without proper rights of access it cannot perform its functions. In the case of an internal oversight by a superior authority, access to information may not be in question. Access to information is more relevant to external oversight.

The Mexican Information Commission[332] and the Slovenian Information Commissioner are responsible for the oversight of the implementation of freedom of information laws. They have the authority to access any classified information. 'Without prejudice to the provisions of the Act governing classified data, the Commissioner (government official) has, without a prior permission, access to classified data'.[333]

Ombudspeople who are responsible for the general oversight of defence and national security entities as regards maladministration, human rights abuses and other wrongdoings, often have also access to classified or privileged information. In the Czech Republic '[t]he following persons may have access to classified information, irrespective of the classification of the information, without the valid PSC [personnel security clearance] and briefing (...) Ombudsman and Deputy Ombudsman'.[334] In New Zealand, the Ombudsmen also have extensive powers to examine any document

> 'In any investigation carried out under this Act pursuant to the Official Information Act 1982 or the Local Government Official Information and

Meetings Act 1987, nothing in subsection (5) prevents an Ombudsman from —

a. requiring, under subsection (1), the furnishing of any information or the production of any document, paper, or thing for which privilege is claimed by any person; and

b. considering the information or inspecting any such document, paper, or thing—

for the purpose of determining whether the information, document, paper, or thing would be properly withheld, but not so as to give the Ombudsman any information, or enable the Ombudsman to make any use of the information, document, paper, or thing that he or she would not, apart from this subsection, be entitled to'. [335]

The European Ombudsman, whose scope of authority covers both matters of right of access to information and maladministration cases within institutions of the European Union, has similar powers. [336]

PRINCIPLE 6

All oversight, ombuds, and appeal bodies, including courts and tribunals, should have access to all information, including national security information, regardless of classification level, relevant to their ability to discharge their responsibilities.
Note: This Principle is expanded upon in Principle 32. It does not address disclosure to the public by oversight bodies. Oversight bodies should maintain the secrecy of all information that has been legitimately classified according to these Principles, as set forth in Principle 35.

14. Archiving national security information

How can one know whether national security information on a specific topic exists? How can one find it?

In every country there is an information management system in the public administration that is of high importance both for the individuals seeking information and the public authorities providing it.[337] The FOI Acts occasionally refer to registers of information held by public bodies, whereas it is fundamental to any secrecy regime to establish registers of classified information. In many countries '[t]he object of such registration is to enable total control over such [classified] documents'.[338] As a matter of course there are systems in which 'compiling an inventory of classified information and equipment is an important part of risk management'.[339] Nonetheless, registers established by FOI Acts do not always contain classified information and the secrecy rules do not always require the registration of all classified information – it is often limited to certain levels of classification. Consequently, two aspects of archiving rules have to be verified: the accessibility of the registers by the public and the range of the registers, i.e. whether the general registers contain references to classified information.

In Sweden, '[o]fficial documents received by an authority or drawn up there must be registered. (...) In order to permit the public ready access to read the registers of authorities, such registers should, in principle, not contain any information subject to secrecy. The authorities may, however, to a certain extent, keep registers with secret information, either as a complement to the public registers or with the permission of the Government (in the Public Access to Information and Secrecy Ordinance)'. There are some exceptions to this rule, among others 'documents that are obviously of little importance to the authorities (...); documents that are obviously of little importance to the authority's activities (for example press cuttings, circulars and advertising material); (...) documents that are found in large numbers at authorities and which the Government has exempted from the registration requirement by special provisions (in the Public Access to Information and Secrecy Ordinance)'.[340]

In Slovenia, a 'catalogue of public information partitioned into content blocks held by the body' shall be continuously maintained and made public in an appropriate manner and a meta-catalogue on catalogues should be published on the internet as well.[341]

PRINCIPLE 15

a. Public authorities have a duty to preserve, manage, and maintain information according to international standards. [2] Information may be exempted from preservation, management, and maintenance only according to law.

b. Information should be maintained properly. Filing systems should be consistent, transparent (without revealing legitimately classified information), and comprehensive, so that specific requests for access will locate all relevant information even if the information is not disclosed.

c. Each public body should create and make public, and periodically review and update, a detailed and accurate list of the classified records it holds, save for those exceptional documents, if any, whose very existence may legitimately be withheld in accordance with Principle 19. *Note: It is good practice to update such lists annually.*

While the registers of the European Parliament, Council and Commission may refer to sensitive documents, *there are sensitive documents which are not recorded.*[342] Those documents which are recorded shall be 'released only with the consent of the originator'.[343] According to Mexican law, '[t]he administrative units shall create, every six months and for each topic, a list including all the files characterized as privileged [classified] or confidential. Said list shall indicate the administrative unit that generated the information, the date of the classification, the grounds, the reserve period, or, if it is the case, those portions of the documents that are privileged or confidential. *This list shall never be deemed as privileged or confidential information'*.[344]

The FOI Act of the United Kingdom does not prescribe the establishment of registers. Rather the Lord Chancellor shall issue and regularly revise a Code of Practice on the Management of Records, which is not binding, but desirable for the public authorities to follow. '[I]f they are failing to comply with the Code, they may also be failing to comply with the Public Records Acts 1958 and 1967, the Local Government (Records) Act 1962, the Local Government Act 1972, the Local Government (Access to Information) Act 1985 or other record-keeping or archives legislation, and they may consequently be in breach of their statutory obligations'.[345]

In Austria, Czech Republic, Estonia, Germany, Poland and Republic of South Africa, there are registers not accesible to the public which may contain the top three levels of classified information or differentiate between levels of protection provided to information of various sensitivities. In Macedonia (FYR), such registers contain all classified information.[346]

Genuinely, if the freedom of information or the secrecy regime has provisions on denial or confirmation of existence of classified information, i.e. allows 'neither deny, nor confirm' responses to access requests, such information which fall into this category are not recorded in the publicly accessible registers.

Although the present study does not cover regulations of historical archives, it has to be noted that in several countries archives may also hold classified records, such as in Australia where

> 'Protectively marked records transferred into the custody of the National Archives of Australia keep the protective markings they had when received from the originating agency and are stored and handled in accordance with those markings. The Archives Act 1983 (the Archives Act), however, provides that where a record is made available for public access in accordance with the Act — in other words, it is in the **open after 30 years period** — and does not contain continuing exempt information, any protective markings cease to have effect fr any purpose'.[347]

RECOMMENDATION

Publicly accessible registers of information held by public bodies can make the information request considerably simpler. This may alleviate the work of public body holding the information as the information requests may become better formulated.

Annexes

Annex I. NATO information standards

Little is known about the information standards of the NATO as only few documents regulating (information) security issues are public. In 2006 the Hungarian National Security Authority disclosed three documents in response to a freedom of information requests by the Hungarian Civil Liberties Union (HCLU), which give the outlines of the NATO's classification system.[1] Presumably the classification system is more complicated, these documents provide only a snapshot into their secrecy regime and there's no publicly available information on their practice. The main documents regulating the classification regime of the NATO is the *C-M(2002)49*, *Security within the North Atlantic Treaty Organisation NATO* (hereinafter: NATO Security Policy) and the *C-M(2002)50, Protection Measures for NATO Civil and Military Bodies, deployed NATO Forces and Installations (Assets) against Terrorist Threats*.[2] The NATO Security Policy is supported by six directives on personnel security, physical security, security of information, industrial security, "Primary Driective on INFOSEC" and "INFOSEC Management Directive for CIS".[3] There is a further document on non-classified information: *The Management of Non-classified NATO Information, C-M(2002)60 which supports the NATO Information Management Policy (NIMP) (PO(99)47).*

According to Enclosure "A" Article 1 (i) of the NATO Security Policy "the Parties shall protect and safeguard classified information, marked as such, which is originated by NATO or which is submitted to NATO by a member state [references omitted]", as well as "classified information, marked as such, of the member states submitted to another member state in support of a NATO programme, project, or contract". These obligations concern only NATO information, but national secrecy regimes have to be adjusted to comply with them and with the very similar EU requirements, detailed below. The NATO Security Policy warns that "NATO security procedures only operate to the best advantage when they are based upon and supported by a national security system having the characteristics" set out in NATO Security Policy.[4] The effects of the NATO Security Policy extend beyond the borders of the member countries as the security agreements are "standard documents" of Partnership for Peace (PfP) nations and „NATO has signed such agreements with most Euro-Atlantic Partnership Council and Mediterranean Dialogue partners".[5] The PfP agreement with Hungary states that the Parties protect each others information and materials according to the agreed common standards, which means in practice a reference to NATO Security Policy as turned out in the court procedure of the HCLU.[6]

The findings of Alasdair Roberts based on the predecessor of the NATO Security Policy are still valid, the system has not changed significantly in the last four decades. Roberts identifies "five basic features, each of which has been adopted with the aim of ensuring a high level of security for information".[7]

---

1 **http://www.freedominfo.org/news/20060921.** htm (01.10.2009), the third document is not published on the website.

2 See C-M(2002)49 at: **http://www.nbf.hu/anyagok/jogszabaly/C-M(2002)49.pdf** (Accessed on 1 October 2009)

3 The Directive on the Security of Information AC/35-D/2002-REV2 is available at: http://www.nbf.hu/anyagok/jogszabaly/AC_35-D_2002-REV2.pdf (Accessed on 1 October 2009)

4 Point 1. of Enclosure „B" to C-M(2002)49

5 http://www.nato.int/cps/en/SID-672B3D9A-62D7A96B/natolive/news_44725.htm?mode=news (Accessed on 7 October 2009)

6 Act V of 1999 on ratification and promulgation of Security Agreement and its Annex on Executive Order, signed by the Government of the Republic of Hungary and NATO on 5th July 1994; 8.Pf.20.969/2007/8. decision of the Metropolitan Court of Appeal in Hungary.

Breadth. The first of these elements might be called the principle of breadth, although this term is not used in NATO documents. It implies that the rules that a member state adopts regarding security of information should govern all kinds of sensitive information, in all parts of government. It eschews narrower approaches, perhaps limited to information received through NATO, or information held within military or intelligence institutions. […]

Depth. The next principle underpinning NATO policy is that of depth of coverage, although again the rule is not expressed in this way in NATO documents. The policy errs on the side of caution when determining what information should be covered by an SOI policy. […]

Centralization. A third principle of NATO policy is that of centralization. This has a national and intergovernmental aspect. At the national level, centralization of responsibility and strong coordination are regarded as "the foundations of sound national security."[reference omitted] Member states are expected to establish a "national security organization" (NSO) that is responsible for the security of NATO information and screening of personnel[…]

Controlled distribution. The NATO security policy invokes two rules that are intended to strictly control the distribution of information. The first of these is "the NEED TO KNOW principle": that individuals should have access to classified information only when they need the information for their work, and access should never be authorized "merely because a person occupies a particular position, however senior." [reference omitted] […]The second rule that restricts the distribution of information might be called the principle of originator control. The principle acknowledges the right of member states, and NATO itself, to set firm limits on the distribution of information that is circulated among member states. […]

Personnel controls. The fifth and final element of the NATO security policy comprises strict rules regarding the selection of individuals who are entitled to view classified information.

---

[7] Roberts, Alasdair S., Entangling Alliances: Nato's Security Policy and the Entrenchment of State Secrecy (October 15, 2002). Cornell International Law Journal, Vol. 36, No. 2, 2003.

Besides these features hardly any of the principles and provisions of national secrecy laws is to be found in the NATO Security Policy.

The protected interests of the NATO which requires these strict rules of protection are not defined, which makes the system prone to arbitrary classifications.

The subjects which may require classification are not defined either.

The lack of expiry of classification is also contrary to the rule of law. Extracts from the Policy on the Public Disclosure of NATO Information on the website of NATO Archives stipulates that "it is the policy of NATO to disclose and make available to the public NATO information that: a) has permanent value and is at least thirty years old; b) has been declassified, if appropriate, by competent authorities in accordance with the NATO Security Policy and its supporting Directives; and c) has been examined by competent authorities in the member nations where required, and approved for public disclosure".[8] These are conjunctive conditions and in this case the usual 30 year rule of archives which provides archival access to 'ordinary documents' at the latest within 30 years of their origination is turned inside out.[9] In this case 30 years is the earliest date to gain access, while there is no time limit to withhold the non-ordinary documents.

NATO Security Policy also deals with the publication of information about civilian installations of military significance. It proposes that "Policy should be designed to hamper the compilation by potential enemies of a Key Points List, to allow the invocation of security exemptions from publication of relevant data".[10] The Programme of Work for Defence Against Terrorism was launched in 2004, presumably realising the policy, but it is unclear how this proposal on invocation of security exemptions was or will be implemented in the national legislations, in the era of Google Earth.[11]

The only feature which can be considered as pro-openness are the restrictions on over-classification. In the NATO system it serves the smooth functioning of the organisation and reduces the costs of physical, personnel, etc. security. The NATO Security Policy prescribes that classified information "shall be managed to ensure that it is appropriately classified […] and remains classified only as long as this is necessary", "when classifying information, the originator shall take account of the damage if the information is subjected to unauthorised disclosure, and shall indicate, where possible, whether their information can be downgraded or declassified on a certain date or event" and "both over-classification and under-classification should be avoided in the interests of effective security as well as efficiency".[12] A rule of thumb against over-classification, which should be followed by national secrecy regimes, is also included "cases of apparent over-classification or under-classification shall be brought to the attention of the originator by the recipient".[13] Which means that not only on review, but any time, by any recipient shall be noted if the classification is not reasonable.

---

[8] **http://www.nato.int/archives/policy.htm** (07.10.2009)

[9] 30 Year Rule Review final report, at: **http://www2.nationalarchives.gov.uk/30yrr/30-year-rule-report.pdf** (07.10.2009)

[10] Point 28. of Enclosure „B" to C-M(2002)49

[11] **http://www.nato.int/docu/update/2007/10-october/e1025e.html** (07.10.2009); **http://www.guardian.co.uk/uk/2006/aug/07/davidleigh.uknews2** (07.10.2009)

[12] Points 16. and 19. of Enclosure „B" to C-M(2002)49 and point 4. of Enclosure „E" to C-M(2002)49

[13] Point 8. of Annex 1 of AC/35-D/2002-REV2

The old principle of Roman law "no delegated powers can be further delegated" is also applied by the NATO Security Policy regarding the authority of classification, which is in this case an element of the controlled distribution feature and it doesn't seem to be originated in the requirement of democratic legitimation.

It is noteworthy that NATO standards became EU standards in few years time after 2000. The way of how NATO's secretive measures were forced through the EU institutions, by circumventing the European Parliament, as well as the Parliaments of the member states, and the struggle of the European Parliament and the civil society for democratic access to information rules in the EU institutions is described in details by Tony Bunyan.[14] The parallel procedure, in which the EU Security Regulations were copied from the 1996 Western European Union Security Regulations by the transmission of NATO security standards is also accurately represented by Martin Reichard.[15] The final EU-NATO agreement on the security of information and relevant security standards don't need further explanation either.[16] What is worth examining at this place, so as to have a better oversight on the international requirements towards national legislations, is the composition of EU secrecy requirements.

Both NATO and the European Union require the establishment of a National Security Authority for the protection of NATO and EU classified information. National Security Authorities have to be set up not only by the member states but also by other countries cooperating with NATO or EU and holding their classified information.[17]

The NATO Security Policy prescribes "the Parties shall ensure the establishment of a National Security Authority for NATO activities which shall implement protective security measures".[18]

The National Security Authority is responsible for (a) the maintenance of security of NATO classified information in national agencies and elements, military or civil, at home or abroad; (b) ensuring that periodic and appropriate inspections are made of security arrangements for the protection of NATO classified information in all national organisations at all levels, both military and civil; (c) ensuring that a security determination of eligibility (security vetting) has been made in accordance with NATO standards with respect to those who are required to access information classified as NATO Confidential and above; (d) ensuring that proper national emergency security plans have been prepared to protect NATO classified information; (e) authorising the establishment of national Cosmic Central Registries.[19]

According to the European Council's security regulations of 2001 within each Member State, a national security organisation shall be set up, which is responsible for "the collection and recording of intelligence on espionage, sabotage, terrorism and other subversive activities, and information and advice to its government, and through it, to the Council, on the nature of the threats to security and the means of protection against them", the

---

[14] Tony Bunyan, CASE STUDY: Secrecy and Openness in the European Union – The Ongoing Struggle for Freedom of Information, at: **http://freedominfo.org/features/20020930.htm** (07.10.2009)

[15] MARTIN REICHARD, THE EU-NATO RELATIONSHIP – A LEGAL AND POLITICAL PERSPECTIVE, 311-352 (Ashgate 2006)

[16] **http://www.statewatch.org/news/2003/jun/10eunato.htm** (07.10.2009)

[17] **http://www.dbki.gov.mk/index_files/home.htm** (20.10.2009); **http://www.alertnet.org/thenews/newsdesk/ISL527603.htm** (20.10.2009)

[18] Article 2 of Enclosure „A" to C-M(2002)49

[19] Point 30 of Enclosure „B" to C-M(2002)49

[20] EU Part I, 5.

same authority shall also "provide information and advice on technical threats to security and the means for protection against them", it collaborates with other government departments and provides recommendations on what information, resources and installations need to be protected, and common standards of protection. [21]

Although these regulations do not impose any obligation on the National Security Authorities which would aim to serve the cause of freedom of information, but the above detailed few pro-openness measures have to be implemented by them. The lawmakers of the NATO and EU member states have to follow these regulations as minimum standards and nothing prevents them to entrust these bodies with more duties, so that the National Security Authorities may also pay particular attention to promoting freedom of information as long as they don't contravene the security requirements.

The provisions regulating the responsibilities Lithuanian Commission for Secrets Protection Co-ordination (NSA) are good examples of the list of duties of NSAs which have relevance with regard to freedom of information, besides the above mentioned tasks. The Lithuanian NSA 1) co-ordinates drafting and implementation of international agreements on protection of classified information; 2) submit proposals to the Government on amending of the present Law and other legal acts related to the protecting of classified information, on their declaring void, and improvement of the current system for the protection of the classified information; 4) analyse and adjust the detailed lists of classified information, related to their activities, drawn up by the subjects of secrets and approve amendments of such lists; 5) decide on expediency of extension of the classifying term; 6) settle disputes between subjects of secrets as well as disputes between subjects of secret and other persons that arise because of classifying, keeping, using, declassifying, control of protection of information considered a State or official secret; 7) under the proposal of the subjects of secrets, decide on the possibilities of transferring classified information to other states or international organisations, other than the contractual parties to agreements on mutual protection of classified information.[22] The Austrian, Czech, Macedonian, New Zealand, Slovene and UK secrecy provisions, as well as a stand-alone Hungarian act entrust the NSAs with similar

---

[21] 2001/264/EC: Council Decision of 19 March 2001 adopting the Council's security regulations

[22] LIT Art 12 para 3.

Annex II: Exceptions to the right of access to information in international human rights treaties

UNIVERSAL DECLARATION OF HUMAN RIGHTS	INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS	EUROPEAN CONVENTION ON HUMAN RIGHTS	INTER-AMERICAN CONVENTION ON HUMAN RIGHTS	COUNCIL OF EUROPE CONVENTION ON ACCESS TO OFFICIAL DOCUMENTS
Article 19 (2) In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.	**Article 19 (3)** The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.	**Article 10 (2)** The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.	**Article 13 (2)** The exercise of the right provided for in the foregoing paragraph shall not be subject to prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure: a. respect for the rights or reputations of others; or b. the protection of national security, public order, or public health or morals	**Article 3 (1)** Each Party may limit the right of access to official documents. Limitations shall be set down precisely in law, be necessary in a democratic society and be proportionate to the aim of protecting: a national security, defence and international relations; b public safety; c the prevention, investigation and prosecution of criminal activities; d disciplinary investigations; e inspection, control and supervision by public authorities; f privacy and other legitimate private interests; g commercial and other economic interests; h the economic, monetary and exchange rate policies of the State; i the equality of parties in court proceedings and the effective administration of justice; j environment; or k the deliberations within or between public authorities concerning the examination of a matter. […] communication with the reigning Family and its Household or the Head of State

Annex III. Categories of Information with a High Presumption in Favour of Disclosure or Overriding Interest in Favour of Disclosure (Principle 10)

Some categories of information, including those listed below, are of particularly high public interest given their special significance to the process of democratic oversight and the rule of law. Accordingly, there is a very strong presumption, and in some cases an overriding imperative, that such information should be public and proactively disclosed.

Information in the following categories should enjoy at least a high presumption in favor of disclosure, and may be withheld on national security grounds only in the most exceptional circumstances and in a manner consistent with the other principles, only for a strictly limited period of time, only pursuant to law and only if there is no reasonable means by which to limit the harm that would be associated with disclosure. For certain subcategories of information, specified below as inherently subject to an overriding public interest in disclosure, withholding on grounds of national security can never be justified.

A. VIOLATIONS OF INTERNATIONAL HUMAN RIGHTS AND HUMANITARIAN LAW

1. There is an overriding public interest in disclosure of information regarding gross violations of human rights or serious violations of international humanitarian law, including crimes under international law, and systematic or widespread violations of the rights to personal liberty and security. Such information may not be withheld on national security grounds in any circumstances.

2. Information regarding other violations of human rights or humanitarian law is subject to a high presumption of disclosure, and in any event may not be withheld on national security grounds in a manner that would prevent accountability for the violations or deprive a victim of access to an effective remedy.

3. When a state is undergoing a process of transitional justice during which the state is especially required to ensure truth, justice, reparation, and guarantees of non-recurrence, there is an overriding public interest in disclosure to society as a whole of information regarding human rights violations committed under the past regime. A successor government should immediately protect and preserve the integrity of, and release without delay, any records that contain such information that were concealed by a prior government. *Note: See Principle 21(c) regarding the duty to search for or reconstruct information about human rights violations.*

4. Where the existence of violations is contested or suspected rather than already established, this Principle applies to information that, taken on its own or in conjunction with other information, would shed light on the truth about the alleged violations.

5. This Principle applies to information about violations that have occurred or are occurring, and applies regardless of whether the violations were committed by the state that holds the information or others.

6. Information regarding violations covered by this Principle includes, without limitation, the following:

    a. A full description of, and any records showing, the acts or omissions that constitute the violations, as well as the dates and circumstances in which they occurred, and, where applicable, the location of any missing persons or mortal remains.

The identities of all victims, so long as consistent with the privacy and other rights of the victims, their relatives, and witnesses; and aggregate and otherwise anonymous data concerning their number and characteristics that could be relevant in safeguarding human rights.
Note: The names and other personal data of victims, their relatives and witnesses may be withheld from disclosure to the general public to the extent necessary to prevent further harm to them, if the persons concerned or, in the case of deceased persons, their family members, expressly and voluntarily request withholding, or withholding is otherwise manifestly consistent with the person's own wishes or the particular needs of vulnerable groups. Concerning victims of sexual violence, their express consent to disclosure of their names and other personal data should be required. Child victims (under age 18) should not be identified to the general public. This Principle should be interpreted, however, bearing in mind the reality that various governments have, at various times, shielded human rights violations from public view by invoking the right to privacy, including of the very individuals whose rights are being or have been grossly violated, without regard to the true wishes of the affected individuals. These caveats, however, should not preclude publication of aggregate or otherwise anonymous data.

b. The names of the agencies and individuals who perpetrated or were otherwise responsible for the violations, and more generally of any security sector units present at the time of, or otherwise implicated in, the violations, as well as their superiors and commanders, and information concerning the extent of their command and control.

c. Information on the causes of the violations and the failure to prevent them.

B. SAFEGUARDS FOR THE RIGHT TO LIBERTY AND SECURITY OF PERSON, THE PREVENTION OF TORTURE AND OTHER ILL-TREATMENT, AND THE RIGHT TO LIFE

Information covered by this Principle includes:

1. Laws and regulations that authorize the deprivation of life of a person by the state, and laws and regulations concerning deprivation of liberty, including those that address the grounds, procedures, transfers, treatment, or conditions of detention of affected persons, including interrogation methods. There is an overriding public interest in disclosure of such laws and regulations.
Notes: "Laws and regulations," as used throughout Principle 10, include all primary or delegated legislation, statutes, regulations, and ordinances, as well as decrees or executive orders issued by a president, prime minister, minister or other public authority, and judicial orders, that have the force of law. "Laws and regulations" also include any rules or interpretations of law that are regarded as authoritative by executive officials.

Deprivation of liberty includes any form of arrest, detention, imprisonment, or internment.

2. The location of all places where persons are deprived of their liberty operated by or on behalf of the state as well as the identity of, and charges against, or reasons for the detention of, all persons deprived of their liberty, including during armed conflict.

3. Information regarding the death in custody of any person, and information regarding any other deprivation of life for which a state is responsible, including the identity of the person or persons killed, the circumstances of their death, and the location of their remains.
Note: In no circumstances may information be withheld on national security grounds that would result in the secret detention of a person, or the establishment and operation of secret places of detention, or secret executions. Nor are there any circumstances in which the fate or whereabouts of anyone deprived of liberty by, or with the authorization, support, or acquiescence of, the state may be concealed from, or otherwise denied to, the person's family members or others with a legitimate interest in the person's welfare.

4. The names and other personal data of persons who have been deprived of liberty, who have died in custody, or whose deaths have been caused by state agents, may be withheld from disclosure to the general public to the extent necessary to protect the right to privacy if the persons concerned, or their family members in the case of deceased persons, expressly and voluntarily request withholding, and if the withholding is otherwise consistent with human rights. The identities of children who are being deprived of liberty should not be made available to the general public. These caveats, however, should not preclude publication of aggregate or otherwise anonymous data.

C. STRUCTURES AND POWERS OF GOVERNMENT

Information covered by this Principle includes, without limitation, the following:

1. The existence of all military, police, security, and intelligence authorities, and sub-units.

2. The laws and regulations applicable to those authorities and their oversight bodies and internal accountability mechanisms, and the names of the officials who head such authorities.

3. Information needed for evaluating and controlling the expenditure of public funds, including the gross overall budgets, major line items, and basic expenditure information for such authorities.

4. The existence and terms of concluded bilateral and multilateral agreements, and other major international commitments by the state on national security matters.

D. DECISIONS TO USE MILITARY FORCE OR ACQUIRE WEAPONS OF MASS DESTRUCTION

1. Information covered by this Principle includes information relevant to a decision to commit combat troops or take other military action, including confirmation of the fact of taking such action, its general size and scope, and an explanation of the rationale for it, as well as any information that demonstrates that a fact stated as part of the public rationale was mistaken.*Note: The reference to an action's "general" size and scope recognizes that it should generally be possible to satisfy the high public interest in having access to information relevant to the decision to commit combat troops without revealing all of the details of the operational aspects of the military action in question (see Principle 9).*

2. The possession or acquisition of nuclear weapons, or other weapons of mass destruction, by a state, albeit not necessarily details about their manufacture or operational capabilities, is a matter of overriding public interest and should not be kept secret.
Note: This sub-principle should not be read to endorse, in any way, the acquisition of such weapons.

E. SURVEILLANCE

1. The overall legal framework concerning surveillance of all kinds, as well as the procedures to be followed for authorizing surveillance, selecting targets of surveillance, and using, sharing, storing, and destroying intercepted material, should be accessible to the public.
Note: This information includes: (a) the laws governing all forms of surveillance, both covert and overt, including indirect surveillance such as profiling and data-mining, and the types of surveillance measures that may be used; (b) the permissible objectives of surveillance; (c) the threshold of suspicion required to initiate or continue surveillance; (d) limitations on the duration of surveillance measures; (e) procedures for authorizing and reviewing the use of such measures; (f) the types of personal data that may be collected and/or processed for national security purposes; and (g) the criteria that apply to the use, retention, deletion, and transfer of these data.

2. The public should also have access to information about entities authorized to conduct surveillance, and statistics about the use of such surveillance.
Note: This information includes the identity of each government entity granted specific authorization to conduct particular surveillance each year; the number of surveillance authorizations granted each year to each such entity; the best information available concerning the number of individuals and the number of communications subject to surveillance each year; and whether any surveillance was conducted without specific authorization and if so, by which government entity.
The right of the public to be informed does not necessarily extend to the fact, or operational details, of surveillance conducted pursuant to law and consistent with human rights obligations. Such information may be withheld from the public and those subject to surveillance at least until the period of surveillance has been concluded.

3. In addition, the public should be fully informed of the fact of any illegal surveillance. Information about such surveillance should be disclosed to the maximum extent without violating the privacy rights of those who were subject to surveillance.

4. These Principles address the right of the public to access information and are without prejudice to the additional substantive and procedural rights of individuals who have been, or believe that they may have been, subject to surveillance.
Note: It is good practice for public authorities to be required to notify persons who have been subjected to covert surveillance (providing, at a minimum, information on the type of measure that was used, the dates, and the body responsible for authorizing the surveillance measure) insofar as this can be done without jeopardizing on-going operations or sources and methods.

5. The high presumptions in favor of disclosure recognized by this Principle do not apply in respect of information that relates solely to surveillance of the activities of foreign governments.
Note: Information obtained through covert surveillance, including of the activities of foreign governments, should be subject to disclosure in the circumstances identified in Principle 10A.

F. FINANCIAL INFORMATION

Information covered by this Principle includes information sufficient to enable the public to understand security sector finances, as well as the rules that govern security sector finances. Such information should include but is not limited to:

1. Departmental and agency budgets with headline items;

2. End-of-year financial statements with headline items;

3. Financial management rules and control mechanisms;

4. Procurement rules; and

5. Reports made by supreme audit institutions and other bodies responsible for reviewing financial aspects of the security sector, including summaries of any sections of such reports that are classified.

G. ACCOUNTABILITY CONCERNING CONSTITUTIONAL AND STATUTORY VIOLATIONS AND OTHER ABUSES OF POWER

This Principle includes information concerning the existence, character, and scale of constitutional or statutory violations and other abuses of power by public authorities or personnel.

H. PUBLIC HEALTH, PUBLIC SAFETY, OR THE ENVIRONMENT

Information covered by this Principle includes:

1. In the event of any imminent or actual threat to public health, public safety, or the environment, all information that could enable the public to understand or take measures to prevent or mitigate harm arising from that threat, whether the threat is due to natural causes or human activities, including by actions of the state or by actions of private companies.

2. (Other information, updated regularly, on natural resource exploitation, pollution and emission inventories, environmental impacts of proposed or existing large public works or resource extractions, and risk assessment and management plans for especially hazardous facilities.

Endnotes

1 Article 19: The Impact of UK Anti-Terror Laws on Freedom of Expression. Submission to ICJ Panel of Eminent Jurists on Terrorism, Counter-Terrorism and Human Rights. April 2006. Available at: http://www.article19.org/data/files/pdfs/analysis/terrorism-submission-to-icj-panel.pdf

2 J Chul Choi, 'Chapter 6: South Korea', in Pal Singh R (ed.), Arms Procurement Decision Making Volume I: China, India, Japan, South Korea and Thailand, 1998

3 The 15 countries with the highest military expenditure in 2011, Stockholm International Peace Research Institute, available at www.sipri.org/research/armaments/milex/resultoutput/milex_15/the-15-countries-with-the-highest-military-expenditure-in-2011-table/at_download/file (accessed 24 April 2012)

4 A Security Strategy for Germany - Resolution of the CDU/CSU Parliamentary Group from May 6, 2008, *available at* www.cducsu.de/GetMedium.aspx?mid=1317 (accessed 24 April 2012); Judy Dempsey, 'Germany Shirks the Big Issue: A Security Strategy' (Carnegie Europe – Strategic Europe), *available at* http://carnegieeurope.eu/strategiceurope/?fa=50111 (accessed 12 June 2013)

5 'Strategic national security objectives in the sphere of state and public security are the protection of Russia's constitutional system, of the basic rights and freedoms of the individual and the citizen, of the sovereignty, independence and territorial integrity of the Russian Federation, and likewise the preservation of civil peace, political and social stability' – Russia's National Security Strategy to 2020 Approved By Decree of the President of the Russian Federation 12 May 2009 No. 537, (unofficial translation), *available at* http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020 (accessed 24 April 2012); 'This Administration has no greater responsibility than the safety and security of the American people' – National Security Strategy of the United States, May 2010, p.4. *available at* www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed 24 April 2012)

6 As of April 2012 China, India, Japan, Saudi Arabia had no publicly accessible national security strategies, Brazil has a published Defence Strategy, but its scope is different to the national security strategies.

7 A Strong Britain in an Age of Uncertainty: The National Security Strategy, HM Government, October 2010, p. 17, *available at* www.direct.gov.uk/nationalsecuritystrategy (accessed 24 April 2012)

8 ibid p. 23.

9 The French White Paper on defence and national security, p.3., *available at* http://www.ambafrance-ca.org/IMG/pdf/Livre_blanc_Press_kit_english_version.pdf (accessed 24 April 2012)

10 La Sala Tercera del Supremo se mantendrá como árbitro en los conflictos sobre secretos, El Mundo, 25 March 1997, *available at* http://web.archive.org/web/20080430171644/http://www.elmundo.es/1997/03/25/espana/25N0019.html (accessed 1 May 2012)

11 "17 octobre 1961', Invisible Paris, 16 October 2011, *available at* http://parisisinvisible.blogspot.co.uk/2011/10/17-octobre-1961.html (accessed 1 May 2012)

12 ALRC Issues Paper 34, Review of Secrecy Laws http://www.austlii.edu.au/au/other/alrc/publications/issues/34/ (accessed 12 June 2013)

13 Law No. 12527 of 18 November 2011, *available at* http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan048795~1.pdf (accessed 1 May 2012)

14 *China to Amend State Secrets Law, Avoid Internet Leakage,* CRIENGLISH.com, 22 June 2009, *available at* http://english.cri.cn/6909/2009/06/22/1821s495548.htm (accessed 12 June 2013)

15 Act CLV of 2009 on Protection of Classified Information, *available at* http://jogszabalykereso.mhk.hu/cgi_bin/njt_doc.cgi?docid=124738.607172 (accessed 29 July 2012)
16 Markus Junianto Sihaloho, *Controversial State Secrecy Bill Comes Back to Life*, Jakarta Globe, *available at* http://www.thejakartaglobe.com/home/controversial-state-secrecy-bill-comes-back-to-life/343234 (accessed 29 July 2012)
17 Shanti Aboobaker and Deon de Lange, *NCOP committee gains three more months to work on Info Bill*, Pretoria News, *available at* http://www.iol.co.za/pretoria-news/ncop-committee-gains-three-more-months-to-work-on-info-bill-1.1323590 (accessed 29 July 2012)
18 Data Secrecy Law, Official Gazette of the Republic of Serbia, No. 104/2009
19 Ukraine Parliament Adopts Access to Information Law, 14 January 2011, *available at* http://www.freedominfo.org/2011/01/ukraine-parliament-adopts-access-to-information-law/ (accessed 1 May 2012)
20 *Global Corruption Report 2003: Access to Information,* Transparency International, 23 January 2003, *available at* http://www.transparency.org/whatwedo/pub/global_corruption_report_2003_access_to_information (accessed 18 February 2013)
21 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001740 Accessed 8 February 2013
22 English translation (2006), at http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Erv&Dokumentnummer=ERV_1987_287
23 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003054 Accessed 8 February 2013
24 http://www.protectivesecurity.gov.au/informationsecurity/Documents/Australian%20Government%20classification%20system.pdf (accessed 4 August 2012)www.nbu.cz/download/nodeid-1859
26 English translation (2008), *available at* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/VSAengl_Fassung_pdf.pdf?__blob=publicationFile (accessed 5 August 2012)
27 http://www.nsa.ee/files/State%20Secrets%20And%20Classified%20Information%20Of%20Foreign%20States%20Act.pdf Accessed 8 February 2013
28 http://www.legislationline.org/documents/id/6835 Accessed 8 February 2013
29 http://www.legaltext.ee/text/en/X40095K2.htm Accessed 8 February 2013
30 http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_e?p_id=157736 Accessed 8 February 2013
31 http://www.dbki.gov.mk/files/pdf_files/Law_on_Classified_Information.pdf Accessed 8 February 2013
32 http://www.freedominfo.org/wp-content/uploads/documents/Macedonia%20FOI%20Law%20ENG%20Official%20Gazette%2013-2006.doc Accessed 8 February 2013
33 English translation *at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB68/laweng.pdf Accessed 8 February 2013
34 http://www.nzsis.govt.nz/publications/Security_in_the_Government_Sector_2002.pdf Accessed 8 February 2013
35 http://www.legislation.govt.nz/act/public/1982/0156/latest/DLM64785.html Accessed 8 February 2013

36 While this study was prepared Poland adopted its new Protection of Classified Information Act of 5 August 2010 which superseded the Classified Information Protection Act of 22 January 1999. Unfortunately no English translation of the new act was available, that's we cannot rely on the text of the law in this study, but Adam Bodnar and Irmina Pacho provide its thorough analysis in their study *'Polish Law on Right to Information and Classification'* (2011) that we used extensively to cover the latest developments in this field in Poland. The study is available at http://right2info.org/resources/publications/national-security-expert-papers/Bodnar_PachoPolishlawonclassification.pdf

37 http://www.right2info.org/resources/publications/laws-1/SA_Minimum%20Information%20Security%20Standards.pdf (accessed 12 June 2013)

38 http://www.justice.gov.za/legislation/acts/2000-002.pdf

39 http://nato.gov.si/eng/documents/classified-info-act/ Accessed 8 February 2013

40 As the text of the Swedish Public Access to Information and Secrecy Act was not available in English we relied on the brochure (http://www.government.se/sb/d/11929/a/131397) produced by the Swedish Ministry of Justice which summarises the act and explains its provisions.

41 http://www.cabinetoffice.gov.uk/sites/default/files/resources/HMG%20Security%20Policy%20Framework%20-%20v8%200%20-%20April%202012.pdf (accessed 5 August 2012)

42 http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information Accessed 8 February 2013

43 See details at: http://www.right2info.org/exceptions-to-access/national-security. As the drafting procedure of the Principles went parallel with the preparation of the present paper therefore not the final version of the Principles could be cited.

44 The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, ARTICLE 19, International Standards Series, November 1996, *available at* http://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf (accessed 12 June 2013)

45 The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, p. 4.; Promotion and protection of the right to freedom of opinion and expression – Report of the Special Rapporteur, Mr. Abid Hussain, pursuant to Commission on Human Rights resolution, UN. Doc. E/CN.4/1996/39 (22 March 1996); Find resolutions of the Commission on Human Rights at: http://www2.ohchr.org/english/bodies/chr/sessions/56/documents.htm

46 See details at: http://right2info.org/exceptions-to-access/national-security#section-3

47 Adopted and opened for signature, ratification and accession by U.N. General Assembly resolution 2200A (XXI) of 16 December 1966, entered into force 23 March 1976.

48 Human Rights Committee, General Comment No 34, Freedoms of Opinion and Expression (Article 19), CCPR/C/GC/34, 12 September 2011, para 21 and 22.

49 Elizabeth Evatt, *The International covenant on Civil and Political Rights: Freedom of Expression and State Security*, in Secrecy and Liberty: National Security, Freedom of Expression and Access to Information 83,88 (Sandra Coliver et al. eds., 1999)

50 *Report of the United Nations High Commissioner for Human Rights and Follow-up to the World Conference on Human Rights,* Human Rights Council, 10th Sess., Agenda Item 2, at 7, A/HRC/10/31/Add.3, (2009)

51 Dr. Agnes Callamard, *Expert meeting on the links between articles 19 and 20 of the ICCPR: Freedom of expression and advocacy of religious hatred that constitutes incitement to discrimination, hostility or violence,* UNHCHR, October 2-3, Geneva, at 5, *at* http://www2.ohchr.org/english/issues/opinion/articles1920_iccpr/docs/experts_papers/Callamard.doc (accessed 19 July 2009)

52 *The Sunday Times v. United Kingdom,* 26 April 1979, Application No. 6538/74, para. 49 (European Court of Human Rights).
53 *Lingens v. Austria*, 8 July 1986, Application No. 9815/82, paras. 39-40 (European Court of Human Rights).
54 This test is used by the Hungarian Constitutional Court – 30/1992. (V. 26.) decision of the Hungarian Constitutional Court
55 Overview of all FOI laws, Roger Vleugels, 9 October 2011, *available at* http://freedominfo.org/documents/Fringe%20Special%20-%20Overview%20FOIA%20-%20oct%202011.pdf (accessed 29 July 2012)
56 Recently this structure was followed by the new Brazilian freedom of information law adopted in 2011.
57 FOI Laws: Counts Vary Depending on Definitions, Toby McIntosh, 28 October 2011, *available at* http://www.freedominfo.org/2011/10/foi-laws-counts-vary-slightly-depending-on-definitions/ (accessed 29 July 2012)
58 Human Rights Committee, General Comment No 34, paragraph 18.
59 Article 17 of the Charter of Fundamental Rights and Basic Freedoms, which is part of the constitutional order of the Czech Republic, *available at* http://www.psp.cz/cgi-bin/eng/docs/laws/1993/2.html (accessed 23 April 2012)
60 Article 61 paragraph 3 of the Constitution of the Republic of Poland, *available at* http://poland.pl/info/information_about_poland/constitution/ch2.htm (accessed 23 April 2012)
61 The form of some regulatory instruments are not clear-cut, therefore their categorisation can be debated. The executive orders in the US provide an example as 'executive orders are generally directed to, and govern actions by, Government officials and agencies. They usually affect private individuals only indirectly', but the 'broad usage of executive orders to effectuate policy goals has led some commentators to suggest that many such orders constitute executive lawmaking that impacts the interests of private citizens and encroaches upon congressional power' in Vanessa K. Burrows, *Executive Orders: Issuance and Revocation,* Congressional Research Service, (March 25, 2010) 1-2, at: https://opencrs.com/document/RS20846/2010-03-25/
62 Though in Mexico there is only one piece of legislation as freedom of information and classification rules are merged in the same Act, it still belongs to the double act model as both issues are regulated by act of the Parliament.
63 In this study examples of those secrecy regimes are obviously not cited where only rules of criminal liability are accessible, but the corpus of classification rules is not public (e.g. China, South Korea).
64 Human Rights Committee, General Comment No 34, paras 24-25
65 *The Sunday Times v. United Kingdom*, 26 April 1979, Application No. 6538/74, para. 49
66 Grayned v. City of Rockford, 408 U.S. 104 (1972), 108-109 (citations omitted)
67 UK2009 p.5.
68 Report of the New Zealand Security Intelligence Service 2003 *available at* http://web.archive.org/web/20081014053220/http://www.nzsis.govt.nz/reports/ar03/review.aspx (accessed 29 July 2012)
69 Information security management guidelines Australian Government security classification system, approved 18 July 2011, *available at* http://www.protectivesecurity.gov.au/informationsecurity/Documents/Australian%20Government%20classification%20system.pdf (accessed 29 July 2012)
70 Sh. Venkatesh Nayak vs M/O Home Affairs on 8 December, 2009, Appeal No. CIC/WB/A/2009/000758 dated 14.08.2008 Right to Information Act 2005 - Section 19, *available at* http://indiankanoon.org/doc/1422672/ (accessed 20 January 2013)

71 34/1994 (VI.24.) decision of the Hungarian Constitutional Court
72 Human Rights Committee, General Comment No 34, paragraph 3.
73 Open legislation and public participation in this field of legislation provide an area for research that has been hardly discovered so far.
74 See the very insightful article of Susan Rose-Ackerman & Benjamin Billa, Treaties and National Security, 40 N.Y.U. J. Int'l L. & Pol. 437 (2008), reprinted in Yale Law School Faculty Scholarship Series, Paper 595, *available at* http://digitalcommons.law.yale.edu/fss_papers/595/
75 AUFOI, Section 11B
76 NZ Chapter 1 para 1 and RSA Chapter 2 para 4
77 SL Art. 2. point 10.
78 MK Art.8.
79 MK Art.8.
80 LIT Art 3 para 4
81 EU Art 2 para 2a
82 old PL Art.2
83 State Secrets and Classified Information of Foreign States Act, Article 3 para 1
84 Bjørn Møller, *National, Societal and Human Security: General discussion with a case study from the Balkans,* Second Round Table, The main challenges facing the promotion of human security and peace in Europe, in UNESCO Division of Human Rights, Democracy, Peace and Tolerance Social and Human Sciences Sector (ed), *International Meeting of Directors of Peace Research and Training Institutions;* Paris; 1st; 2000; What agenda for human security in the twenty-first century? Publ: 2001; 41-62,, *available at* http://www.unesco.org/securipax/whatagenda.pdf (accessed 12 June 2013)
85 Office of the Australian Information Commissioner's Guide to the Freedom of Information Act 1982 (November 2011), 46, *available at* http://www.oaic.gov.au/publications/agency_resources/guide_freedom_of_information_act_1982.pdf (accessed 4 August 2012)
86 ibid, p.48.
87 MXr Art 26
88 SL Art. 11
89 Toby Mendel, *Freedom of information: a comparative legal survey* (2nd rev. ed., UNESCO 2008;2009) 36, *available at* http://portal.unesco.org/ci/en/ev.php-URL_ID=26159&URL_DO=DO_TOPIC&URL_SECTION=201.html (accessed 18 February 2013).
90 Damage usually refers to economic damage, see SW 3.6.2
91 old EST Art. 5 to 7. – In the former Estonian law the legislator would not entrust the public officials with assessing the possible harms or threats of unauthorised access, but divided different topics of state secrets into three categories of increasing importance, under the presumption that any piece of information belonging to a topic always needs the same level of protection and there is always a danger present which justifies the classification.
92 UK2009 p.24.
93 SL Art. 11
94 NZ Annex C-F '**Restricted:** • Affect diplomatic relations adversely. • Hinder the operational effectiveness or security of New Zealand or friendly forces. • Affect the internal stability or economic well-being of New Zealand or friendly countries adversely. **Confidential:** • Materially damage diplomatic relations (i.e. cause formal protest or other sanctions). • Cause damage to the operational effectiveness or security of New Zealand or friendly forces or to the continuing effectiveness of valuable security or intelligence operations. • Damage the internal stability of New Zealand or friendly countries. • Disrupt significant national infrastructure. **Secret:** • Raise international tension. •Damage seriously relations with friendly governments. • Cause serious damage to the operational

effectiveness or security of New Zealand or friendly forces or the effectiveness of valuable security or intelligence operations. • Seriously damage the internal stability of New Zealand or friendly countries. • Shut down or substantially disrupt significant national infrastructure. **Top Secret:** • Threaten directly the internal stability of New Zealand or friendly countries. • Lead directly to widespread loss of life. • Cause exceptionally grave damage to the operational effectiveness or security of New Zealand or friendly forces or the effectiveness of extremely valuable security or intelligence operations. • Cause exceptionally grave damage to relations with other governments. • Cause severe long-term damage to significant national infrastructure'.

95 new PL Art 5

96 old PL Art 2.

97 LIT Art 2

98 EU Art 2 para 1

99 new HU Art 3 point 1a

100 AUINFOSEC, 3.1

101 MK Art.8.

102 The Council of Europe Convention on Access to Official Documents in its article 3.2 allows restrictions if the disclosure 'would or would be likely to harm' protected interests, *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/205.htm (accessed 8 February 2013)

103 Public Interest Declassification Board, *Transforming the Security Classification System* (December 2012) 9, *available at* http://www.archives.gov/declassification/pidb/recommendations/transforming-classification.html (accessed 18 February 2013).

104 1087 (1996) Resolution on the consequences of the Chernobyl disaster of the Parliamentary Assembly of the Council of Europe; The link between contaminated milk and censorship, Amnesty International, *available at* http://www.amnesty.org.au/china/comments/17761/ (accessed 12 June 2013)

105 AU2007 1.6.3.1.2 (reference omitted)

106 There is public interest test **concerning sensitive (classified) information** in Australia, Estonia (only concerning internal information related to an offence or accident – ESTFOI Art 38 para 1), Macedonia (MKFOI Art 6 para 3), New Zealand (NZFOI Part 1 Section 9), Republic of South Africa (RSAFOI Section 46(b), Slovenia (SLFOI Art 6 para 2), Sweden, United Kingdom (UKFOI Section 2 para 2 and Art 17 para 3) and there is no public interest test concerning sensitive (classified) information in Austria (according to Art 1 para 1 of the AFOI information can be given only to the 'extent not being in contradiction to a statutory duty of secrecy' which is contrary to any test), Czech Republic, European Union, Germany, Hungary, Lithuania, Mexico and Poland.

107 EUFOI Art 4(1)(a) and Art. 9; SLFOI Art 6 para 2

108 UKFOI Section 2

109 UKFOI Section 2 para 3

110 Information Commissioner's Office Guidance on Section 24: the national security exemption, version 1, 1 June 2009, p.5., *available at* http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/s24_national_security_v1_fop098.pdf and Freedom of Information Act Awareness Guidance No. 10 - The Defence Exemption, version 1, April 2006, *available at* http://www.ico.gov.uk/for_organisations/guidance_index/freedom_of_information_and_environmental_information.aspx#exemptions (accessed 18 February 2013)

111 SW 3.8

112 RSAFOI Section 46(b) and NZFOI Part 1 Section 9

113 AU2007, 1.6.3.1

114 Australian Information Commissioner's Guide, pp. 50-51.

115 Information Commissioner's Office, Freedom of Information Act Awareness Guidance No. 10 – The Defence Exemption, *available at* http://www.ico.gov.uk/for_organisations/guidance_index/~/media/documents/library/Freedom_of_Information/Detailed_specialist_guides/AWARENESS_GUIDANCE_10_-_THE_DEFENCE_EXEMPTION.ashx (accessed 5 August 2012)
116 SLFOI Art 6 para 2
117 ESTFOI Art 38 para 1
118 MKFOI Art 6 para 3
119 old PL Art 2 para 2
120 CZr
121 old HU Art 4 para 4
122 'Information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security in accordance with section 1.2 of this order, and it pertains to one or more of the following: (a) military plans, weapons systems, or operations; (b) foreign government information; (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology; (d) foreign relations or foreign activities of the United States, including confidential sources; (e) scientific, technological, or economic matters relating to the national security; (f) United States Government programs for safeguarding nuclear materials or facilities; (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or (h) the development, production, or use of weapons of mass destruction.' - Executive Order 13526 - Classified National Security Information, December 29, 2009, Part 1, Section 1.4, *available at* http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information, (accessed 25 April 2012)
123 Executive Order 13526 - Classified National Security Information, December 29, 2009, Part 1, Section 1.9
124 Information Security Oversight Office, Fundamental Classification Guidance Review, *available at* http://www.archives.gov/isoo/fcgr/
125 AUINFOSEC, Annex A
126 SW 2.2
127 ALRC Issues Paper 34 Review of Secrecy Laws Appendix 2. Table of Secrecy Provisions, *available at* http://www.austlii.edu.au/au/other/alrc/publications/issues/34/9.html (accessed 12 June 2013) (emphasis added)
128 Recommendation 1792 (2007) Fair trial issues in criminal cases concerning espionage or divulging state secrets, *available at* http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta07/EREC1792.htm
129 HMG Security Policy Framework, May 2009, version 2.0
130 MK Art. 5.
131 LIT Art 2
132 D Art 2.
133 State Secrets Act, passed on 26 January 1999 (RT* I 1999, 16, 271), Art. 19. para 5., *available at* http://www.legislationline.org/documents/action/popup/id/6835 (accessed 25 April 2012)
134 UK2012 pp.22-23.
135 EU Art 2.
136 Vasiliy Mitrokhin, KGB Lexicon: The Soviet Intelligence Officer's Handbook, 366 (Frank Cass & Co. Ltd 2002)
137 Rosamund Thomas, Espionage and Secrecy: The Official Secrets Acts 1911-1989 of the United Kingdom (Routledge 1991)
138 NZ Chapter 4 para 63; MX Art. 17.

139 UK2012 p.24.
140 D Art 8 para 1 commentary
141 NZ Chapter 3 paras 20-23; The manual has further recommendations to reduce over-classification: 'Where appropriate and practical, organisations should: • encourage staff to challenge questionable classifications; • have line managers check classifications routinely; • in security instructions, clearly define how the Chief Executive or head delegates authority for classification;• in complex documents such as books, reports, memoranda or minutes of meetings, separately classify each chapter, section, page or paragraph; this can be indicated by inserting the appropriate classification in parentheses immediately following the section or paragraph number or in the sideline if unnumbered; • avoid rules for automatic classification, as they can result in documents bearing classifications higher than warranted'. - NZ Chapter 3 point 24
142 D Art 8. para 2
143 LIT Art 2 para 31
144 NZ Chapter 3 para 6
145 Guidelines issued by the Australian Information Commissioner under s93A of the Freedom of Information Act 1982, Part 5, point 5.23, *available at* http://www.oaic.gov.au/publications/guidelines/Guidelines-s93A-FOI-Act_Part5_Exemptions.pdf (accessed 4 August 2012)
146 UK2009, p.17.; N.B. the relationship of the Data Protection Act 1998 (DPA) and the Protective Marking System is similar. 'Whilst the DPA makes no reference to the Protective Marking System, protective markings may be a helpful indicator that an exemption applies. The presence, or absence, of a protective marking is not in itself a deciding factor as to whether or not information should be released in response to a subject access request, but it may nevertheless provide some initial guidance as to whether and which exemption applies'. – UK2009, p. 19.
147 UK2012, p.9.
148 RSA Chapter 1 paras 3 and 4
149 Sandy Africa, *Well-kept Secrets - The right of access to information and the South African intelligence services* (Institute for Global Dialogue and Friedrich-Ebert-Stiftung 2009) 83 *available at* http://library.fes.de/pdf-files/bueros/suedafrika/07162.pdf (accessed 18 February 2013)
150 DFOI Art 3 para 4
151 Art 4 of Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes, at http://www.gesetze-im-internet.de/s_g/__4.html (accessed 12 June 2013)
152 See for example the UN Human Rights Committee's Concluding observations on Uzbekistan (CCPR/CO/71/UZB), para 18. which points out that 'the Committee is particularly concerned about the definition of "State secrets and other secrets" as defined in the Law on the Protection of State Secrets. It observes that the definition includes issues relating, inter alia, to science, banking and the commercial sector and is concerned that these restrictions on the freedom to receive and impart information are too wide to be consistent with article 19 of the Covenant'.
153 See for example the Memorandum of the President of the USA (December 29, 2005) on Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, *available at* http://www.fas.org/sgp/isoo/guidelines.html (accessed 18 February 2013)
154 Roberts, Alasdair S., Entangling Alliances: Nato's Security Policy and the Entrenchment of State Secrecy (October 15, 2002). Cornell International Law Journal, Vol. 36, No. 2, 2003, 14-15, (citations omitted), *available at* http://ssrn.com/abstract=1307692 (accessed 18 February 2013)

155 new EST Art 26
156 old PL Art 49 para 1 see changes in Polish legislation in Bodnar-Pacho, 17-21
157 'Participants in pre-trial proceedings or judicial proceedings, an individual involved in the proceedings and the representatives of both parties in criminal, civil or administrative matters, or matters of misdemeanour have the right to access, after passing the security vetting, state secrets classified as 'restricted', 'confidential' or 'secret' on the basis of a reasoned order of an investigative body, the Prosecutor's office or a court ruling if access is unavoidably necessary for the adjudication of the criminal, civil or administrative matter, or the matter of misdemeanour.' - new EST Art 26 para 1
158 Of course the lack of reference in other secrecy laws does not necessarily mean that in these legal systems there are no provisions at all on handling classified information in court procedures, but unfortunately the detailed examination of these questions would go beyond the scope of this study.
159 Point 2. of ENCLOSURE "F" to Security Within The North Atlantic Treaty Organisation (NATO) , C-M(2002)49, *available at* http://www.nbf.hu/jogszab.html (accessed 18 February 2013)
160 EU Art 5
161 Rethinking Classification: Better Protection and Greater Openness in *Report of the Commission on Protecting and Reducing Government Secrecy (*1997) 19 *available at* http://www.gpo.gov/fdsys/granule/GPO-CDOC-105sdoc2/GPO-CDOC-105sdoc2-7/content-detail.html (accessed 18 February 2013)
162 SW 3.5.4
163 SW 2.3
164 In the terminology of protection of classified information rules collectively called media.
165 Council of Europe Convention on Access to Official Documents (ETS No. 205) *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/205.htm (accessed 18 February 2013)
166 NZ Chapter 3 para 24
167 US EO 13526, Part 1, Sec. 1.6, c) and g)
168 Department of Justice Guide to the Freedom of Information Act (2009), 82-83 n.221-222 (citations and footnotes omitted), *available at* http://www.justice.gov/oip/foia_guide09/procedural-requirements.pdf (accessed 18 February 2013)
169 UK2012 p.24.
170 UK2012 p.24., see also D Art 6 para 1; EU Art 4 para 4; new EST Art 17; new HU Art 9 para 5 (regarding foreign classified information); MK Art 11; NZ Chapter 4 para 92; old PL Art 19 para 3; RSA Chapter 4 para 1.5; SL Art 14;
171 Pozen, David E., The Mosaic Theory, National Security, and the Freedom of Information Act. Yale Law Journal, Vol. 115, pp. 628-679, 2005.
172 D Anlage 1. point 1.; SL Art 14; old PL Art 19 para 3;
173 Point 8. of Enclosure 'E' to Security Within The North Atlantic Treaty Organisation (NATO) , C-M(2002)49, *available at* http://www.nbf.hu/jogszab.html (accessed 18 February 2013)
174 EU Annex III, title II, section 7. – In the preceding EU regulation (Council Decision of 19 March 2001 adopting the Council's security regulations (2001/264/EC), Section XI Chapter V para 51.) the same risk was framed as 'It shall be incumbent upon an organisation and its information holders to consider the problems of aggregation of individual elements of information, and the inferences that can be gained from the related elements, and determine whether or not a higher classification is appropriate to the totality of the information'.
175 Australian Information Commissioner's Guidelines, Part 5, point 5.34
176 Vereiniging Weekblad Bluf! vs. The Netherlands of Feb 9, 1995, series A, No.

306-A, (Application no. 16616/90)
177 RSA Chapter 4 para 1.6
178 For U.S. case-law see Phillippi v. CIA, 546 F.2d 1009 (D.C. Cir 1976)
179 Non-Paper - Regulation of the European Parliament and of the Council regarding Public Access to European Parliament, Council and Commission documents, SN 5249/00, *available at* http://database.statewatch.org/e-library/2000-5249-non-paper-atd.pdf (accessed 18 February 2013)
180 UKFOI Section 1
181 Awareness guidance 21 of the United Kingdom's Information Commissioner on The duty to confirm or deny, *available at* http://www.ico.org.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/awareness_guidance_21_-_the_duty_to_confirm_or_deny.pdf (accessed 12 June 2013)
182 Guidance of the United Kingdom's Information Commissioner on Section 24: the national security exemption of the Freedom of Information Act, *available at* http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/s24_national_security_v1_fop098.pdf (accessed 12 June 2013)
183 LIT Art 2 para 1
184 NZFOI Part 1 Section 10
185 SL Art 19
186 UKFOI Section 1 para 1 and practically every exemption has provisions referring to it.
187 AUFOI, Section 25
188 Australian Information Commissioner's Guidelines, Part 5, point 5.44, http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-3&chapter=4&lang=en (accessed on 27 January 2013)
190 Human Rights Committee, General Comment No 34, Freedoms of Opinion and Expression (Article 19), CCPR/C/GC/34, 12 September 2011, para 19.
191 Case of Taxquet v. Belgium (Application no. 926/05), Judgement of 13 January 2009, § 43
192 In an earlier decision the ECtHR declared that '[f]or Article 6, paragraph (1) (art. 6-1), (...) covers all proceedings the result of which is decisive for private rights and obligations. The English text "determination of ... civil rights and obligations", confirms this interpretation. The character of the legislation which governs how the matter is to be determined (civil, commercial, administrative law, etc.) and that of the authority which is invested with jurisdiction in the matter (ordinary court, administrative body, etc.) are therefore of little consequence.' -- Case of Ringeisen v. Austria (Merits) (Application no 2614/65) § 94
193 AU2007, 'Using these Guidelines', p.5
194 Executive Order 13526- Classified National Security Information, December 29, 2009, Part 1, Section 1.1. b), *available at* http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information, (accessed 18 April 2012)
195 Office of the Australian Information Commissioner, Guidelines under s 93A of the Freedom of Information Act 1982 (2010).
196 Freedom of Information Guidelines – Exemption Sections in the FOI Act , Prepared for the Department of the Prime Minister and Cabinet as at 9 October 2009, para 1.6.2 (references to case-law omitted), *available at* www.dpmc.gov.au/foi/docs/FOI_act_exemptions.doc (accessed 18 April 2012)
197 Classified Information Act, Art. 11, *available at* http://nato.gov.si/eng/documents/classified-info-act/, (accessed 18. April 2012)

198 Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung - VSA) vom 31. März 2006, Anlage 1 point 1, *available at* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/VSA_pdf.pdf?__blob=publicationFile, (accessed 18. April 2012)

199 Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Art. 17, *available at* http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf , (accessed 18. April 2012) and Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Art. 30, *available at* http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFTAIPG.pdf, (accessed 18. April 2012)

200 new HU, Art 6 para (2)-(3)

201 Australian Law Reform Commission, Review of Secrecy Laws (2008), 30-31, available at http://www.austlii.edu.au/au/other/alrc/publications/issues/34/IP34.pdf (accessed 12 June 2013)

202 Guidance of the Information commissioner on Section 24 of the Freedom of Information Act http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/s24_national_security_v1_fop098.pdf (accessed 18 February 2013)

203 Philip Coppel, *The Freedom of Information Act 2000 and related rights,* Judicial Studies Board, (2007), 11

204 Ministerial veto on disclosure of Cabinet minutes concerning military action against Iraq, Information Commissioner's Report to Parliament, at http://www.ico.gov.uk/upload/documents/library/freedom_of_information/research_and_reports/ico_report_on%20iraq_minutes_ministerial_veto.pdf (accessed 12 June 2013)

205 Judith Bannister, *A tale of two tax stories; Freedom of Information and determining the public interest in Australia and the United Kingdom, Open Government: a journal on freedom of information* [Online], Volume 4 Number 1, at http://www.opengovjournal.org/article/view/2648/2052 (accessed 12 June 2013)

206 Freedom of Information (Removal of Conclusive Certificates and Other Measures) Act 2009

207 Freedom of Information Guidelines – Exemption Sections in the FOI Act, 1.7

208 NZFOI Section 6

209 Official information legislation guides Part 2B, Office of the Ombudsman, *available at* http://www.ombudsman.parliament.nz/system/paperclip/document_files/document_files/174/original/part_2b__conclusive_reasons.pdf?1344201712

210 NZFOI Section 31

211 http://www.lawcom.govt.nz/project/review-official-information-act-1982-and-local-government-official-information-act-1987

212 The works of Franz Kafka or the study of Max Weber (WIRTSCHAFT UND GESELLSCHAFT, 730 (Köln/Berlin 1964)) may give answers to the questions regarding its origin.

213 National Archives, About Controlled Unclassified Information (CUI), *available at* http://www.archives.gov/cui/

214 First Annual CUI Report to the President, *available at* http://www.archives.gov/cui/reports/report-2011.pdf

215 MK Art 10

216 ESTFOI Art 35 para 1

217 UK2009 p. 22 and 27 – this rule has been slightly simplified by UK2012 (p. 24) as 'Any material originating outside of government that is not covered by a recognised protective marking, but is marked to indicate sensitivity, must be handled and protected to at least the level offered by the PROTECT marking', but the details of the earlier text better shows the approach applied in this field.

218 NZ Chapter 3 para 13
219 NZ Chapter 3 para 6
220 Decision 12/2004 (IV.7.) AB, *available at* http://www.mkab.hu/letoltesek/en_0012_2004.pdf (accessed 18 February 2013)
221 In the Hungarian FOI law data and information are synonyms.
222 Public Access to Information and Secrecy with Swedish Authorities (2004), 25, *available at* http://www.freedominfo.org/documents/Sweden%20public%20access%20to%20info%202004.pdf (accessed 18 February 2013)
223 SW 2.2
224 Executive Order 11652, *available at* http://fas.org/irp/offdocs/eo/eo-11652.htm (accessed 12 June 2013)
225 AUINFOSEC, 3.6
226 Executive Order 13526 - Classified National Security Information, December 29, 2009, Part 1, Section 1.7
227 John M. Ackerman, *Mexico's Freedom of Information Law in International Perspective,* in Mexico's Right-to-Know Reforms 314,314 (Jonathan Fox et al. eds., 2007) (reference omitted and emphasis added)
228 MXr Art 36
229 UN Human Rights Council, *Joint study on secret detention of the Special Rapporteur on torture & other cruel, inhuman or degrading treatment or punishment, the Special Rapporteur on the promotion and protection of human rights & fundamental freedoms while countering terrorism, the Working Group on Arbitrary Detention & the Working Group on Enforced or Involuntary Disappearances ,* 19 February 2010, A/HRC/13/42, 129, 131, *available at* http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-42.pdf
230 ibid 131-132
231 SL Art 6 and MK Art 20
232 RSA Chapter 2 point 3.4
233 INFCIRC/335 (18 November 1986) and INFCIRC/336 (18 November 1986)
234 Report of the Parliamentary Assembly of the Council of Europe: The consequences of the Chernobyl disaster, Doc. 7538, 24 April 1996, point 4.1, *available at* http://assembly.coe.int/ASP/XRef/X2H-DW-XSL.asp?fileid=16498&lang=EN
235 Find the convention at http://www.unece.org/fileadmin/DAM/env/pp/documents/cep43e.pdf
236 Find more details in The Implementation Guide to the Aarhus Convention, United Nations Economic Commission for Europe, ECE/CEP/72, 2000, *available at* http://www.unece.org/env/pp/acig.html
237 ibid 71.
238 UKFOI Section 23
239 Freedom of Information Act 1982, Section 7 and Division 1 of Part I of Schedule 2, *available at* http://www.austlii.edu.au/au/legis/cth/consol_act/foia1982222/
240 Act CXII of 2011 On Informational Self-determination and Freedom of Information, Article 2 para 1, (note data is used as synonym of information) , see unofficial translation at: http://naih.hu/files/ACT_2011_CXII_in_eng-v2.pdf (accessed 24. April 2012)
241 The Freedom of Information Act – Act of 11 May 1999 n. 106/1999 Coll. on free access to information (July 2011 up to date version), Article 2, *available at* http://www.otevrete.cz/en/the-freedom-of-information-act-with-signed-changes-by-amendment-from-2006-153.html (accessed 24. April 2012)

242 Federal Act Governing Access to Information held by the Federal Government (Freedom of Information Act) of 5 September 2005 (Federal Law Gazette [BGBl.] Part I, p. 2722), Section 3 subsection 8, *available at* http://www.gesetze-im-internet.de/englisch_ifg/englisch_ifg.html (accessed 24. April 2012)
243 SW 2.2
244 On the origins of these three principles find more details in Roberts, Alasdair S., Entangling Alliances: Nato's Security Policy and the Entrenchment of State Secrecy (October 15, 2002). Cornell International Law Journal, Vol. 36, No. 2, 2003. Available at SSRN: http://ssrn.com/abstract=1307692
245 The expression 'author' is also used for originator (see Chapter 2 para 2 of RSA), however the public official creating and classifying information may be two individuals which might lead to confusion in terminology if it is not recognised by the law.
246 SL Art 10, MK Art 9
247 new EST Art 27 para 5
248 CZ Section 58 para 1 d
249 old HU Art 6 para 1
250 RSA Chapter 4 para 1
251 SL Art 10, MK Art 9
252 RSA Chapter 2 para 14; SL Art 10
253 NZ Chapter 3 para 18
254 OpenTheGovernment.org, Secrecy Report 2012, 19, *available at* http://www.openthegovernment.org/sites/default/files/Secrecy2012_web.pdf (accessed 18 February 2013)
255 Employee's Guide to Security Responsibilities, Defense Personnel Security Research Center, May 2006, version 3.0, *available at* http://www.dhra.mil/perserec/csg/s1class/classif.htm
256 old PL Art 22; new PL Art 19
257 UK2012, p. 15.
258 NZ Chapter 3 para 23, D Art 11 para 2
259 Rethinking Classification: Better Protection and Greater Openness (1997) 21
260 NEW YORK TIMES CO. v. UNITED STATES, 403 U.S. 713 (1971) *available at:* http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=403&invol=713
261 D Art 42
262 new EST Art 13 para 4
263 AUINFOSEC, 3.4
264 UK2009, p. 20
265 Ar Art 3 para 2; CZ Section 22 para 7; D Art 9 para 1; new HU Art 8 para 3; LIT Art 7 para 3; MK Art 14; old PL Art 21 para 5; RSA chapter 4 para 1.4.1; SL Art 18;
266 old EST Art 9 para 3
267 CZ Section 22 para 5; new HU Art 8 para 1
268 EU Annex III para 16
269 MK Art 19
270 D Anlage 6 point 4.2
271 NZ Chapter 3 para 33
272 State Secrets And Classified Information Of Foreign States Act, Article 13 para 2
273 old EST Art 11 para 4
274 LIT Art 8
275 MX Art 15
276 old PL Art 21 para 5; new PL Art 9
277 Bodnar-Pacho, 26
278 Bodnar-Pacho 26, citing an interview with Piotr Niemczyk

279 SL Art 21
280 AUINFOSEC, 3.9
281 Kenedi v. Hungary, (Application no. 31475/05) §45
282 new EST Art 24 para 2
283 D Anlage 8 para 3 point 4
284 CZ Section 146
285 Until the abolishment of the position of Parliamentary Commissioner of Personal Data Protection and Freedom of Information the Commissioner had this power and from 1 January 2012 the National Authority for Data Protection and Freedom of Information is authorised to gain access and perform such review.
286 CZ Section 58 para 1
287 Decision of the European Parliament on the regulations and general conditions governing the performance of the Ombudsman's duties, Article 3 para 2
288 Ombudsmen Act 1975, Article 19
289 Public Protector Act 23 of 1994, Article 7 para 4a
290 MX Art 17
291 HUFOI Art 63.
292 SLFOI Art 6, Art 21, Art 27
293 SLFOI Art 31
294 The criminal law provisions attached to disclosure or unauthorised access to classified information is a highly important issue concerning the exercise of freedom of expression and freedom of information. Criminal provisions also mean the ultimate response if the state of the classification system fails to provide adequate protection to sensitive information. The current study does not cover criminal issues, as Miklós Haraszti (OSCE Representative on Freedom of the Media) and David Banisar (Director of the FOI Project of Privacy International, London), in an extensive study, already described the legal environment and key issues in the member states of the OSCE in 2007. Find details in: Access to information by the media in the OSCE region: trends and recommendations, *available at* http://www.osce.org/fom/24892 and Access to information by the media in the OSCE region: Country Reports, *available at* http://www.osce.org/fom/24893 (24. July 2012)
295 Case of the Slovenian Information Commissioner No: 090-29/2009, May 4, 2009 Časopisna hiša Dnevnik d.d. (News publisher Dnevnik), vs. decision of the Slovenian Government
296 old EST Art 9 para 2
297 NZ Chapter 3 para 33
298 Vereiniging Weekblad Bluf! vs. The Netherlands of Feb 9, 1995, series A, No. 306-A §38 §45 (citations omitted)
299 EU Art 13 para 4
300 34/1994 (VI.24.) decision of the Hungarian Constitutional Court
301 LIT Art 5 para 4
302 NZ Chapter 4 para 126-128
303 D Anlage 8 Art 2
304 MX Art 47
305 Antonio Gonzalez Quintana, Archives of the Security Services of Former Repressive Regimes report prepared for UNESCO on behalf of the International Council of Archives, (UNESCO 1997)
306 Recommendation No. R (2000) 13 of the Committee of Ministers to member states on a European policy on access to archives, at https://wcd.coe.int/ViewDoc.jsp?id=366245 (accessed 12 June 2013); Council of Europe Convention on Access to Official Documents also applies to archives see point 15. of the Explanatory Report, at http://conventions.coe.int/Treaty/EN/Reports/Html/205.htm (accessed 12 June 2013);

307 Most of these reports should be available in English as English and French are the official languages of the NATO. Nine NSAs have websites on their own. Czech Republic, Estonia, Hungary, Lithuania, Poland and Slovenia are NATO members which presumably prepare reports on the activities of NSA in English. The NSAs of Australia, New Zealand and the Republic of South Africa also have websites and English is official language in these countries. Macedonia is partner of the NATO and the website of the NSA has a very detailed English version without their annual reports. Find the Czech Report at http://www.nbu.cz/en/other-documents/ and the Polish report at http://www.abw.gov.pl/portal/en/16/577/Annual_report_2009.html (accessed 18 February 2013)
308 http://www.archives.gov/isoo/; http://www.archives.gov/declassification/pidb/ (accessed 18 February 2013)
309 Access to Information Programme, *Access to Information in Bulgaria 2011 Report* (2012) 17 *available at* http://store.aip-bg.org/publications/ann_rep_eng/2011.pdf (accessed 18 February 2013)
310 MX Art 15
311 US EO Part 1 Sec 1.5 b)
312 AUINFOSEC, 3.8
313 LIT Art 8 para 7
314 Bodnar-Pacho, 28-29
315 new EST Art 8
316 Act CLV of 2009 on Protection of Classified Information, Article 5 para 7, SW 3.6.2
317 D Art 9 para 3
318 Bodnar-Pacho, 10
319 old PL Art 25 para 2
320 new EST Article 9 para 2
321 NZ Chapter 4 para 126
322 D Art 9 para 3; LIT Art 6 para 5; MX Art 15; US Part 3 Sec. 3.3
323 old HU Art 28 para 2, new HU Art 39 paras 1-2
324 National Security Information, Executive Order 12065 (June 28, 1978), *available at* http://www.fas.org/irp/offdocs/eo/eo-12065.htm (accessed 18 February 2013)
325 Executive Order 12958 on Classified National Security Information, Sec 3.4 a) *available at* http://www.fas.org/sgp/clinton/eo12958.html (accessed 18 February 2013)
326 Steven Aftergood, 'Congress Resists Efforts to Reduce Secrecy' (*Secrecy News*, 6 August 2012) *available at* http://www.fas.org/blog/secrecy/2012/08/congress_resists.html (accessed 18 February 2013)
327 AU2007 1.3.5
328 MX Art 14, MXr 37
329 new PL Art 1 para 3
330 D Art 9 para 1 commentary
331 Access to Information by Intelligence and Security Service Oversight Bodies, Aidan Wills and Benjamin S. Buckland, DCAF, OSF 2012, *available at* http://www.dcaf.ch/Publications/Access-to-Information-by-Intelligence-and-Security-Service-Oversight-Bodies (accessed 24. April 2012)
332 Federal Transparency and Access to Public Government Information Law, Article 45, *available at* http://www.ifai.org.mx/descargar.php?r=/pdf/english/&a=LFTAIPG%20ENG%202010.pdf (accessed 25. April 2012)
333 Act on revisions and additions to the Act on access to public information (ZDIJZ-A) (Official gazette of RS, no. 61-2663/2005), published 30.6.2005, Article 31, *available at* https://www.ip-rs.si/index.php?id=324 (accessed 25. April 2012)

334 Act N. 412 of 21 September 2005 on the Protection of Classified Information, Art 58 para 1, *available at* www.nbu.cz/download/nodeid-1814/ (accessed 25. April 2012)
335 Ombudsmen Act 1975, Article 19, para 5A
336 Decision of the European Parliament on the regulations and general conditions governing the performance of the Ombudsman's duties, Article 3, *available at* http://www.ombudsman.europa.eu/en/resources/statute.faces (accessed 25. April 2012)
337 Helen Darbishire & Thomas Carson, Transparency and Silence - a Survey of Access to Information Laws and Practices in 14 Countries, 120 (Stephen Humphreys et al. eds., Open Society Institute, 2006)
338 RSA Chapter 4 para 3.2
339 NZ Chapter 3 para 2
340 SW 3.4.2
341 SLFOI Art 8
342 Special Report from the European Ombudsman to the European Parliament following the draft recommendation to the Council of the European Union in complaint 917/2000/GG, *available at* http://www.ombudsman.europa.eu/cases/specialreport.faces/en/382/html.bookmark (accessed 12 June 2013)
343 EUFOI Art 9 para 3
344 MX Art 17 (emphasis added)
345 UKFOI Section 46, Lord Chancellor's Code of Practice on the Management of Records under Section 46 of the Freedom of information Act 2000, 4-5 (November 2002), *available at* http://www.justice.gov.uk/downloads/information-access-rights/foi/foi-section-46-code-of-practice.pdf (accessed 5 August 2012)
346 Ar Art 11.; CZ Section 21, Section 137 (e); D Art 18 para 1; new EST Art 36 para 2 ('Registration of copies made of classified media, except the media containing state secret classified as "restricted" or "confidential", is mandatory'.); RSA Chapter 4 point 3.2; MK Art 63; Bodnar-Pacho, 11-12.
347 AUINFOSEC, 3.5, as the Australian Information Commissioner's Guide (page 16) points out 'The Archives Act has also been changed as part of this legislative reform package. The open access period in the Archives Act, which defines the age at which most government information is released to the public, is being reduced from 30 years to 20 years (and from 50 years to 30 years for Cabinet documents). This change is being phased in over a 10-year period, commencing on 1 January 2011. All Australian Government agencies, including security intelligence agencies that are excluded from the operation of the FOI Act, fall under the Archives Act'. excluded from the operation of the FOI Act, fall under the Archives Act.

Classified Information

Report author: Ádám Földes

Editor: Saad Mustafa

Design: SVI Design, Maria Gili

This report has been printed on FSC certified paper.

ISBN number: 978-0-9927122-0-4

Transparency International UK
32-36 Loman Street
London SE1 0EH
United Kingdom

© Transparency International UK
All rights reserved.

First published in April 2014.

Reproduction in whole or in parts is permitted, providing that full credit is given to Transparency International UK (TI-UK) and provided that any such reproduction, in whole or in parts, is not sold or incorporated in works that are sold.

Effort has been made to verify the accuracy of the information contained in this report. Nevertheless, Transparency International UK cannot accept responsibility for the consequences of its use for other purposes or in other contexts.

Transparency International UK's Defence and Security Programme works to reduce corruption in defence and security worldwide.

We engage with governments, armed forces, security forces, defence companies, international organisations, civil society and others to advance this goal.

We provide new tools, practical reforms, benchmarks and research to enable change.