

# Access to Information and Security Sector Governance



Amin  
Media  
Network



Geneva Centre for the  
Democratic Control of  
Armed Forces (DCAF)

Reference Text Reader

# Access to Information and Security Sector Governance

## About DCAF

The Geneva Centre for the Democratic Control of Armed Forces (DCAF) promotes good governance and reform of the security sector. The Centre conducts research on good practices, encourages the development of appropriate norms at the national and international levels, makes policy recommendations and provides in-country advice and assistance programmes. DCAF's partners include governments, parliaments, civil society, international organisations and security sector actors such as police, judiciary, intelligence agencies, border security services and the military.

DCAF has worked in the Palestinian Territories since 2005. It assists a wide range of Palestinian actors such as ministries, the Palestinian Legislative Council, civil society organisations and the media in their efforts to make Palestinian security sector governance democratic, transparent and accountable.

## About AMIN

Established in 1996, the AMIN Media Network is a non-profit Palestinian organisation which promotes the development of media. AMIN supports the participation of professional media in building a democratic society based on the principles of freedom of expression, transparency and objectivity. AMIN also works to strengthen the relationship between local media and civil society organisations. In this framework, AMIN assesses the needs of the local media institutions and seeks to propose solutions to overcome their difficulties. Further information on AMIN is available at: [www.amin.org](http://www.amin.org)

## Note

This publication has been produced with the financial assistance of the Spanish Agency for International Development Cooperation (AECID: Agencia Española de Cooperación Internacional para el Desarrollo). The contents of this publication are the exclusive responsibility of the Geneva Centre for the Democratic Control of Armed Forces (DCAF) and do not necessarily reflect the opinion of AECID.

## Editorial Board

Munjed Abdallah  
Khaled Abu Aker  
Azzam Abu Baker  
Taghreed Abu Hamdah  
Mahmud Alawneh  
Majed Arouri  
Prof. Bertil Cottier  
Roland Friedrich  
Pascal Gemperli  
Regula Kaufmann  
Jonas Loetscher  
Arnold Luethold  
Nicolas Masson  
Salah Moussa  
Said Zaid

## Design and Layout

Wael Dwaik

## Translation Support

Intissar Abu Khalaf  
Rania Filfil  
Yaseen N. Al-Sayyed

## Language editing

Garance Stettler

## Publisher

Geneva Centre for the Democratic Control of Armed Forces (DCAF)  
Rue de Chantepoulet 11  
P.O. Box 1360  
1211 Geneva 1  
Switzerland

Tel: +41 (22) 741 77 00  
Fax: +41 (22) 741 77 05

[www.dcaf.ch](http://www.dcaf.ch)

Cover Picture: © Nicolas Masson / Citizen consults official documents at the Headquarters of the Palestinian National Security Forces, Ramallah, 2010

ISBN: 978-92-9222-132-4

© DCAF 2010. All rights reserved.

# **Table of contents**

<b>Introduction</b>	<b>4</b>
<b>Part I:</b> <b>National Legislation</b>	<b>11</b>
Sweden: Freedom of the Press Act; Chapter 2: On the Public Nature of Official Documents (1978)	12
Mexico: Federal Transparency and Access to Public Government Information Law (2002)	16
Switzerland: Law on the Principle of Transparency in the Federal Administration (2005)	20
Palestinian National Authority: Draft Law on the Right to Access Information (2005)	25
<b>Part II:</b> <b>Standards Promoted by Regional and International Bodies</b>	<b>33</b>
Commonwealth Freedom of Information Principles (1999)	34
Council of Europe Convention on Access to Official Documents (2009)	35
<b>Part III:</b> <b>Standards Promoted by Non-Governmental Organisations</b>	<b>43</b>
The Johannesburg Principles on National Security, Freedom of Expression and Access to Information (1996)	44
Principles on Freedom of Information Legislation, Article 19, Global Campaign for Free Expression (1999)	49

# Introduction

## What is access to information?

Access to information is foremost a fundamental human right. It is enshrined in Article 19 of the Universal Declaration of Human Rights (1948):

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

This right of access to information contains two dimensions. First, it compels the government to publish and disseminate to the public key information about what different public bodies are doing. Second, it obliges the government to receive from the public requests for information and to respond to them. Today, more than 80 countries around the world have adopted comprehensive access to information (ATI) – or freedom of information (FOI) – legislation.

### Box 1: Elements of an access to information law

Article 19, a London based human rights organisation, has drawn up a set of principles on what should go into an access to information law.<sup>1</sup> The principles contained in the list are recognised by many countries as being the standard for best practice on this issue. The following is a slightly amended list of Article 19 list of principles governing an access to information law:

- Access to information legislation should be guided by the principle that all information held by public bodies can be accessed by members of the public (principle of maximum disclosure)

- Exceptions should be clearly and narrowly drawn
- Public bodies should be under an obligation to publish key information
- Public bodies must actively promote open government
- Requests for information should be processed rapidly and fairly and an independent review of any refusals should be available
- Any refusal of access to information must be motivated in writing
- Individuals should not be deterred from making requests for information by excessive costs
- Laws that are inconsistent with the principle of maximum disclosure should be amended or repealed
- Individuals who release information on wrongdoing - whistleblowers - must be protected.

<sup>1</sup> Source: <http://www.article19.org/work/regions/latin-america/FOI/english/elements/index.html>

## Why is access to information important?

In democratic countries, it is important that people have access to a wide range of official information. Information allows people to make informed decisions about their own lives. Access to information also enhances debates and discussions on public affairs and allows people to participate in the decision-making processes of government. Access to information also allows the media and civil society to provide

checks and balances on the government, the military and other powerful sectors in society. It exposes vested interests, identifies corrupt officials and encourages a level playing field. In countries with a recent history of human rights abuses, access to information allows redress of past harm. By exposing past abuses, access to information also prevents repetitions in the future.

#### **Box 2: Why access to information is important for the Council of Europe**

“Transparency of public authorities is a key feature of good governance and an indicator of whether or not a society is genuinely democratic and pluralist, opposed to all forms of corruption, capable of criticising those who govern it, and open to enlightened participation of citizens in matters of public interest. The right of access to official documents is also essential to the self-development of people and to the exercise of fundamental human rights.”

Source: Commentary to Council of Europe Convention on Access to Official Documents (CETS 205), 2009

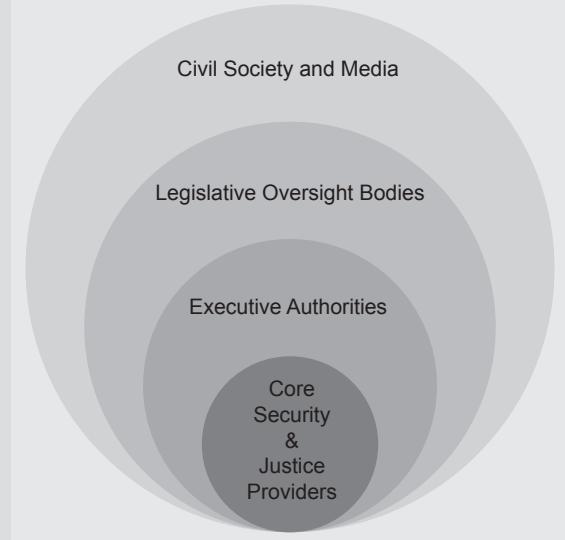
### **Why is access to information important for good governance of the security sector?**

Good governance of the security sector requires that the core security and justice providers and their oversight and management bodies (see: security sector chart) operate in a transparent way. They also must be accountable to the people and their elected representatives for their performance and conduct. In this regard, access to government records and information held by the government, the armed forces, the police, and the security forces is an essential requirement to ensure transparency and accountability.

In turn, governments and the armed forces, the police, and the security forces can benefit from access to information as well. Access to information forces them to setup record keeping and archiving systems. This, in turn, improves efficiency and allows making better decisions based on factual information. Finally, greater transparency builds trust between the government and its citizens.

### **What is the Security Sector?**

Legal & Policy Framework



The security sector consists of the core security and justice providers and their management and oversight institutions. The legal and policy framework regulates their tasks, authorities and structures.

#### **Core security and justice providers:**

- Security forces (armed forces, police, intelligence and security services, but also liberation armies and insurgency groups)
- Justice and law enforcement institutions (courts, prosecution services, prisons, traditional justice systems)

#### **Management and oversight institutions:**

- Executive management and oversight bodies (Presidency, Council of Ministers, ministries of defence, interior, justice and finance)
- Legislative management and oversight bodies (Parliament and its committees, ombudspersons)
- Informal oversight institutions (civil society organisations, media, research and advocacy organisations)

### **Does access to information mean that all government records can be accessed?**

No. Access to information is a fundamental but not an absolute right. International standards recognise that there are legitimate reasons for restricting access to information, which, if released, would cause harm. For example, to release all information about an ongoing police criminal inquiry to the public might harm the possibility that the police will catch the criminal suspect. After the enquiry is finished and the criminal arrested, the information could be released.<sup>1</sup> Today, every access law includes exemptions to the right of access to information. Limitations often concern one or several of the following areas:<sup>2</sup>

- National security, defence and international relations
- Public safety
- The prevention, investigation and prosecution of criminal activities
- Disciplinary investigations
- Inspection, control and supervision by public authorities
- Privacy and other legitimate private interests
- Commercial and other economic interests
- The economic, monetary and exchange rate policies of the State
- The equality of parties in court proceedings and the effective administration of justice
- Environment
- The deliberations within or between public authorities concerning the examination of a matter.

However, it is important to stress that this does not necessarily mean that all information related to these areas should be kept secret. For example, in most countries, public bodies are obliged to black out or otherwise remove the sensitive information and give you the rest of the document. If the information is in electronic form, then the sensitive information can be removed. However, in that case, the public body should indicate that “editing” had been done and mark where that was. Furthermore, the public body should justify in detail why it was necessary.<sup>3</sup>

### **What are the criteria for deciding which information should be kept secret?**

There are no universally accepted standards on what constitute legitimate reasons for restriction on access to information. Furthermore, each country needs to take into account its specific political, economic and cultural context. However, there are three principles which are increasingly accepted by states in this regard;

- *Prescribed by law:* Restrictions on access to information must be prescribed by law. The law must be accessible, unambiguous, drawn narrowly and with precision so as to enable individuals to foresee whether a particular action is unlawful.

The law should provide for adequate safeguards against abuse, including prompt, full and effective judicial scrutiny of the validity of the restriction by an independent court or tribunal.

- *Necessary in a democratic society:* To establish that a restriction on access to is necessary to protect legitimate interests, a government must demonstrate that:

- the information at issue poses a serious threat to a legitimate interest;
- the restriction imposed is the least restrictive means possible for protecting that interest; and

<sup>1</sup> Example taken from What Is the Right to Know?, Access Info. Available at: <http://www.access-info.org/en/what-is-the-right-to-know/44>

<sup>2</sup> Based on the exemptions as listed in the Council of Europe Convention on Access to Official Documents (CETS 205), 2009.

<sup>3</sup> Adapted from Exceptions to the Access to Information, Access Information. Available at: <http://www.access-info.org/en/what-is-the-right-to-know/44>.

- the restriction is compatible with democratic principles.
- *Proportionate:* Any restriction must be proportionate to the aim of protecting other legitimate rights and interests.

## **Does access to information undermine national security and public order?**

One of the most frequent arguments made against access to information is that it undermines national security and public order. However, it can also be argued that better access to information enhances national security and public order:<sup>4</sup>

- *Access to information helps keeping security and intelligence forces focused on threats to national security:* In many countries, the various agencies responsible for 'national security' spend a lot of their time monitoring and repressing legitimate political opposition groups. Access to information on their work helps keeping security and intelligence forces focused on national security threats as outlined in national defence and security policy documents.
- *Access to information fosters political stability:* Some governments misuse pretexts of threats to national security to maintain their own grip on power. In the absence of access to information, governments can be tempted to warn of plots and conspiracies organised by perceived enemies of the state in order to keep popular opposition at bay. However, there is a risk that such a strategy creates a backlash by fostering frustration among the people and promoting a climate of fear and mistrust in the country. In turn, better access to information discourages government bodies to issue false information. In this sense, access to information can foster political stability.

- *Access to information reduces feelings of exclusion and unjust treatment:* In countries with minorities or strong political divisions, minorities or opposition groups may accuse the government that they are being unfairly treated. In turn, better access to information allows people to scrutinise decisions personally. This helps reducing tensions and causes of conflict.

## **What criteria should governments apply when restricting access to information related to national security and public order?**

Pretexts of national security and public order are often misused in order to protect information that might reveal:

- Breaches of human rights;
- Corruption within public authorities;
- Administrative errors;
- Information which is simply embarrassing for public officials or public authorities.

In 1995, a group of experts in freedom of speech and information met in Johannesburg, South Africa to reflect on the relationship between national security and access to information. The group developed principles that became known as the Johannesburg Principles on National Security, Freedom of Expression and Access to Information. Since they were released in 1996, these principles have been endorsed by many international and regional organisations, including the UN, the Organisation of American States (OAS) and the Organisation for Security and Cooperation in Europe (OSCE).

<sup>4</sup> Adapted from: Arguments For/Against FOI, Article 19. Available at: <http://www.article19.org/work/regions/latin-america/FOI/english/arguments/2.html#against4>.

### Box 2: Johannesburg Principles on National Security, Freedom of Expression and Access to Information (1996)

The most important provisions of the Johannesburg Principles on National Security, Freedom of Expression and Access to Information (1996) related to access to information include:

**Principle 11: General Rule on Access to Information:** Everyone has the right to obtain information from public authorities, including information relating to national security. No restriction on this right may be imposed on the ground of national security unless the government can demonstrate that the restriction is prescribed by law and is necessary in a democratic society to protect a legitimate national security interest.

**Principle 12: Narrow Designation of Security Exemption:** A state may not categorically deny access to all information related to national security, but must designate in law only those specific and narrow categories of information that it is necessary to withhold in order to protect a legitimate national security interest.

**Principle 13: Public Interest in Disclosure:** In all laws and decisions concerning the right to obtain information, the public interest in

knowing the information shall be a primary consideration.

**Principle 14: Right to Independent Review of Denial of Information:** The state is obliged to adopt appropriate measures to give effect to the right to obtain information. These measures shall require the authorities, if they deny a request for information, to specify their reasons for doing so in writing and as soon as reasonably possible; and shall provide for a right of review of the merits and the validity of the denial by an independent authority, including some form of judicial review of the legality of the denial. The reviewing authority must have the right to examine the information withheld.

**Principle 15: General Rule on Disclosure of Secret Information:** No person may be punished on national security grounds for disclosure of information if (1) the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or (2) the public interest in knowing the information outweighs the harm from disclosure.

Note: A full version of these principles is available on pp. 44-48 of this Reader.

## What are the challenges to improve access to information in the Palestinian Territories?

*"In the Palestinian context, access to information is a human right. Yet, in practice, the right of access to information is not granted in Palestine. Security reasons are invoked to deprive citizens from this right."*

Staffer of the Palestinian Legislative Council (PLC), DCAF-AMIN workshop, March 2010

Since the establishment of the Palestinian National Authority (PNA) in 1994, members of the Palestinian Legislative Council (PLC) as well as civil society and media representatives have made many attempts to promote the adoption of a Palestinian law on access to information. The PLC debated a draft law in 2005 but never adopted it.

Today, Palestinian civil society and media representatives try to promote transparency, accountability and access to information in security sector governance. In doing so, they are facing a number of challenges. The most important ones are:

- The restrictive legal and regulatory framework governing the Palestinian security sector;<sup>5</sup>
- The lack of trust between Palestinian security personnel, the media and civil society organisations; and

<sup>5</sup> For instance, Art. 90 [10] of the Law of Service in the Palestinian Security Forces No. 8 (2005) and Art. 35 [3] of the General Intelligence Law No. 17 (2005) restrict Palestinian security officers' right to provide information related to their work. See Quneis, Juman: "The Palestinian Media and Security Sector Legislation", in: The Palestinian Media and Security Sector Governance, DCAF, 2009, pp. 11-13.

- A culture of secrecy among the authorities and the core security and justice providers.<sup>6</sup>

In addition, representatives of the PNA and its security forces often invoke matters of ‘national security’ and ‘public order’ to restrict public access to information. Yet, as these terms are not clearly defined, Palestinian civil society and media practitioners are often hesitant to cover topics related to the operations, management, long-term strategies and budgets of the security forces. Those who attempt to cover internal or external conflicts and security incidents are often targeted by the security forces.<sup>7</sup>

## Toward adopting access to information legislation in the Palestinian Territories

Against this background, the Geneva Centre for the Democratic Control of Armed Forces (DCAF) and AMIN Media Network conducted a joint project entitled ‘Strengthening Palestinian Security Sector Governance Through Better Access to Information’. Between January and May 2010, DCAF and AMIN organised four workshops in Ramallah, bringing together 20 representatives of the Palestinian security forces, the Ministries of Justice and the Interior, the Palestinian Legislative Council (PLC), the Judiciary, civil society, the media, and independent researchers. The workshops assessed the challenges and potential opportunities to enhance Palestinian citizens’ and media’s access to information related to the Palestinian security sector. Media and civil society practitioners agreed that more efforts should be made to enhance transparency and accountability in Palestinian security sector governance and reform. They formulated the following recommendations to enhance access to information held by Palestinian security sector institutions:

- Adopt a Law on Access to Information;

<sup>6</sup> See DCAF Spotlight No. 5 (December 2009): Assessing the Role of Media in Palestinian Security Sector Governance, p. 2.

<sup>7</sup> In 2009, the Palestinian Center for Development and Media Freedoms (MADA) has counted 173 violations of media freedoms in the Palestinian Territories.

- Promote procedures for the filing, classification and de-classification of records held by Palestinian security sector institutions;
- Foster a dialogue and establishing communication channels between civil society representatives, the media and representatives of the PNA and its security forces;
- Devise mechanisms to oversee the implementation of access to information; and
- Strengthen the role of the media in order to promote an informed debate on Palestinian security sector governance and reform.

## What is the purpose of this reader?

This reader aims to provide Palestinian practitioners with international legislation on access to information. The texts have been selected to inspire Palestinian lawmakers to develop their own legislation to promote transparency in security sector governance. More specifically, this reader aims to:

- Provide the PLC, civil society and the media, as well as the Palestinian security forces with reference laws on access to information;
- Invite them to study and compare existing access to information legislation with a view to understanding the prevailing practices in other democratic countries;
- Introduce the legal procedures that various countries have developed to ensure transparency and accountability in security sector governance; and
- Foster an informed debate about the importance of promoting public access to security-related information among Palestinian stakeholders.

## **How is this reader structured?**

The first section of this reader contains the Palestinian Draft Law on the Right to Access Information as well as access to information laws from various democratic countries. The second section presents regional and international standards on access to information. The third section introduces access to information standards that have been elaborated by Article 19, one of the main non-governmental organisations working to promote free access to information worldwide.

# **Part I**

# **National Legislation**

# **Sweden: The Freedom of the Press Act (1978)<sup>8</sup>**

[...]

## **Chapter 2. On the public nature of official documents**

### **Art. 1**

Every Swedish citizen shall be entitled to have free access to official documents, in order to encourage the free exchange of opinion and the availability of comprehensive information.

### **Art. 2**

The right of access to official documents may be restricted only if restriction is necessary having regard to

1. the security of the Realm or its relations with another state or an international organisation;
2. the central fiscal, monetary or currency policy of the Realm;
3. the inspection, control or other supervisory activities of a public authority;
4. the interest of preventing or prosecuting crime;
5. the economic interest of the public institutions;
6. the protection of the personal or economic circumstances of private subjects;
7. the preservation of animal or plant species.

Any restriction of the right of access to official documents shall be scrupulously specified in a provision of a special act of law, or, if this is

deemed more appropriate in a particular case, in another act of law to which the special act refers. With authority in such a provision, the Government may however issue more detailed provisions for its application in a statutory instrument.

The provisions of paragraph two notwithstanding, the Riksdag or the Government may be empowered, in a regulation under paragraph two, to permit the release of a particular document, having regard to the circumstances.

### **Art. 3**

Document is understood to mean any written or pictorial matter or recording which may be read, listened to, or otherwise comprehended only using technical aids. A document is official if it is held by a public authority, and if it can be deemed under Article 6 or 7 to have been received or drawn up by such an authority.

A recording under paragraph one is deemed to be held by a public authority, if it is available to the authority using technical aids, which the authority itself employs, for communication in such form that it may be read, listened to, or otherwise comprehended. A compilation of information taken from material recorded for automatic data processing is however regarded as being held by the authority only if the authority can make it available using routine means.

A compilation of information taken from material recorded for automatic data processing is not however regarded as being held by the authority if the compilation contains personal information and the authority is not authorised in law, or under a statutory instrument, to make the compilation available. Personal information is understood to mean any information which

<sup>8</sup> The following is an extract of the Swedish Freedom of Press Act. A full version is available at: [http://www.riksdagen.se/templates/R\\_Page\\_\\_\\_\\_6313.aspx](http://www.riksdagen.se/templates/R_Page____6313.aspx)

can be referred back directly or indirectly to a private person.

**Art. 4**

A letter or other communication which is directed in person to an official at a public authority is deemed to be an official document if it refers to a case or other matter falling within the authority's purview, and if it is not intended for the addressee solely in his capacity as incumbent of another position.

**Art. 5**

The Riksdag and any local government assembly vested with decisionmaking powers is equated with a public authority for the purposes of this Chapter.

**Art. 6**

A document is deemed to have been received by a public authority when it has arrived at the authority or is in the hands of a competent official. A recording under Article 3, paragraph one, is instead deemed to have been received by the authority when it has been made available to the authority by another in the manner indicated in Article 3, paragraph two.

Competition documents, tenders and other such documents which it has been advertised shall be delivered under sealed cover are deemed not to have been received before the time appointed for their opening.

Measures taken solely as part of the technical processing or technical storage of a document which a public authority has made available shall not be construed to mean that the document has been received by that authority.

**Art. 7**

A document is deemed to have been drawn up by a public authority when it has been dispatched. A document which has not been dispatched is deemed to have been drawn up when the matter to which it relates has been finally settled by the authority, or, if the document does not relate to a specific matter, when it has been finally checked and approved by the authority, or has otherwise received final form.

The provisions of paragraph one notwithstanding, a document of the nature referred to below is deemed to have been drawn up:

1. in the case of a day book, ledger, and such register or other list as is kept on an ongoing basis, when the document has been made ready for notation or entry;
2. in the case of a court ruling and other decision which shall be pronounced or dispatched under relevant provisions of law, and records and other documents insofar as they relate to such a decision, when the decision has been pronounced or dispatched;
3. in the case of other records and comparable memoranda held by a public authority, when the document has been finally checked and approved by the authority or has otherwise received final form, but not the records of Riksdag committees, auditors of local authorities, official commissions of inquiry or local authorities where they relate to a matter dealt with solely in order to prepare the matter for decision.

**Art. 8**

If a body which forms part of, or is associated with, a public authority or other similar organisation for the public administration has transferred a document to another body within the same organisation, or has produced a document for the purpose of transferring it in this manner, the document is not deemed thereby to have been received or drawn up, other than if the bodies concerned act as independent entities in relation one to the other.

**Art. 9**

Neither shall a memorandum which has been prepared at a public authority, but which has not been dispatched, be deemed to be an official document at that authority after the time at which it would be deemed to have been drawn up under Article 7, unless it has been accepted for filing and registration. Memorandum is understood to mean any aide memoire or other note or record produced solely for the preparation or oral presentation of a matter,

## **Access to Information and Security Sector Governance**

but not such part of it as contributes factual information to the matter.

Preliminary outlines or drafts of decisions or written communications of a public authority and other like documents which have not been dispatched are not deemed to be official documents unless they have been accepted for filing and registration.

### **Art. 10**

A document held by a public authority solely for the purpose of technical processing or technical storage on behalf of another is not deemed to be an official document held by that authority.

### **Art. 11**

The following documents are not deemed to be official documents:

1. letters, telegrams, and other such documents delivered to or drawn up by a public authority solely for the purpose of forwarding a communication;
2. notices or other documents delivered to or drawn up by a public authority solely for the purpose of publication in a periodical published under the auspices of the authority;
3. printed matter, recordings of sound or pictures, or other documents forming part of a library or deposited by a private person in a public archive solely for the purpose of care and safe keeping, or for research and study purposes, and private letters, written matter or recordings otherwise transferred to a public authority solely for the purposes referred to above;
4. recordings of the contents of documents under point 3, if such recordings are held by a public authority, where the original document would not be deemed to be an official document.

The provisions of paragraph one, point 3, concerning documents forming part of a library do not apply to recordings held in databases to which a public authority has access under an agreement with another public authority, if the recording is an official document held by that authority.

### **Art. 12**

An official document to which the public has access shall be made available on request forthwith, or as soon as possible, at the place where it is held, and free of charge, to any person wishing to examine it, in such form that it can be read, listened to, or otherwise comprehended. A document may also be copied, reproduced, or used for sound transmission. If a document cannot be made available without disclosure of such part of it as constitutes classified material, the rest of the document shall be made available to the applicant in the form of a transcript or copy.

A public authority is under no obligation to make a document available at the place where it is held, if this presents serious difficulty. Nor is there any such obligation in respect of a recording under Article 3, paragraph one, if the applicant can have access to the recording at a public authority in the vicinity, without serious inconvenience.

### **Art. 13**

A person who wishes to examine an official document is also entitled to obtain a transcript or copy of the document, or such part thereof as may be released, in return for a fixed fee. A public authority is however under no obligation to release material recorded for automatic data processing in any form other than a printout except insofar as follows from an act of law. Nor is a public authority under any obligation to provide copies of maps, drawings, pictures, or recordings under Article 3, paragraph one, other than in the manner indicated above, if this would present difficulty and the document can be made available at the place where it is held.

Requests for transcripts or copies of official documents shall be dealt with promptly.

### **Art. 14**

A request to examine an official document is made to the public authority which holds the document.

The request is examined and approval granted by the authority indicated in paragraph one. Where special grounds so warrant, it may however be laid down in a provision under Article 2, paragraph two, that in applying this

rule, examination and approval shall rest with another public authority. In the case of a document of central significance for the security of the Realm, it may also be laid down in a statutory instrument that only a particular authority shall be entitled to examine and approve questions relating to release. In the aforementioned cases, the request shall be referred to the competent authority forthwith.

No public authority is permitted to inquire into a person's identity on account of a request to examine an official document, or inquire into the purpose of his request, except insofar as such inquiry is necessary to enable the authority to judge whether there is any obstacle to release of the document.

#### **Art. 15**

Should anyone other than the Riksdag or the Government reject a request to examine an official document, or release such a document with a proviso restricting the applicant's right to disclose its contents or otherwise dispose over it, the applicant may appeal against the decision. An appeal against a decision by a minister shall be lodged with the Government, and an appeal against a decision by another authority shall be lodged with a court of law.

The act referred to in Article 2 shall set out in greater detail how an appeal against a decision under paragraph one shall be lodged. Such an appeal shall always be examined promptly.

Special provisions apply to the right to appeal against decisions by authorities under the Riksdag.

#### **Art. 16**

A note concerning obstacles to the release of an official document may be made only on a document covered by a provision under Article 2, paragraph two. Such a note shall refer to the relevant provision.

#### **Art. 17**

It may be laid down in law that the Government, or a local government assembly vested with decision-making powers, may determine that official documents relating to the activities of a public authority which are to be taken over by a private body may be transferred into the

safe keeping of that body, if it requires the documents for its work, without the documents ceasing thereby to be official. Such a body shall be equated with a public authority in respect of documents so transferred when applying Articles 12 to 16.

It may also be laid down in law that the Government may determine that official documents may be transferred to the Church of Sweden, or any part of its organisation, for safe keeping, without the documents ceasing thereby to be official. This applies to documents received or drawn up no later than 31 December 1999 by

1. public authorities which no longer exist and which performed tasks relating to the activities of the Church of Sweden; or
2. decision-making assemblies of the Church of Sweden.

In applying Articles 12 to 16, the Church of Sweden and any part of its organisation shall be equated with a public authority in respect of documents so transferred.

#### **Art. 18**

Basic rules concerning the storage of official documents, weeding and other disposal of such documents are laid down in law.

[...]

# Mexico: Federal Transparency and Access to Public Government Information Law (2002)<sup>9</sup>

[...]

## Chapter II

### The obligations of transparency

#### Article 7

With the exception of classified or confidential information as stipulated in this Law, the subjects compelled by the Law must, under the terms of the Regulations and guidelines that the Institute or an equivalent instance as specified in Article 61 produces, put at the public's disposition and keep up to date the following information:

- I. Their constitutional structure;
- II. The powers of each administrative unit;
- III. A directory of their public servants, from the level of the head of the department or his equivalent and below;
- IV. The monthly remuneration received for each position, including the system of compensation as established in the corresponding dispositions;
- V. The address of the liaison section, as well as the electronic address where requests for information can be received;
- VI. The aims and objectives of the administrative units according to their operational schemes;
- VII. The services they offer;
- VIII. Their procedures, requisites and forms. When these are inscribed in the Federal Register of Procedures and Services or in

the Register established by the Secretariat of the Treasury and Public Credit for tax purposes, they must be published exactly as they are registered;

- IX. Information concerning the budget assigned to each agency, as well as reports about its disbursement, in the terms established by the Budget for the Federation's Expenses. In the case of the Executive Branch, this information will be made available for each agency and entity by the Secretariat of the Treasury and Public Credit, which will also inform the public about the economic situation, public finance and the public debt in the terms established by the budget;
- X. The results of the audit of any subject compelled by the Law completed, as appropriate, by the Secretariat of the Comptroller and Administrative Development, internal comptrollers or the Federation's Superior Auditor, and, in such cases, the corresponding explanations;
- XI. The design and execution of subsidy programs as well as the amounts allocated to them and criteria for access to them.
- XII. All concessions, permits or authorizations granted, with their recipients specified.
- XIII. All contracts granted under the terms of the applicable legislation detailing for each contract:
  - a) The public works, goods acquired or rented, and the contracted service; in the case of studies or research the specific subject must be indicated;
  - b) The amount;

<sup>9</sup> The following is an extract of the Mexican Transparency and Access to Public Government Information Law. A full version is available at: <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB68/laweng.pdf>

- c) The name of the provider, contractor or the physical or moral person to whom the contract has been granted, and
  - d) The periods within which the contracts must be completed.
- XIV. The norms applicable to each subject compelled by the Law.
- XV. The reports that each subject must generate, according to the law.
- XVI. Mechanisms for citizen participation in cases where they exist, and
- XVII. Any other information that may be useful or considered relevant, in addition to information based on statistical surveys that is responsive to the public's most frequently asked questions.

The information to which this article refers must be made public in such a form as to facilitate its use and comprehension by individuals, and ensure its quality, veracity, timeliness and trustworthiness. The agencies and entities must refer to the recommendations made by the Institute in this regard.

### **Article 8**

The Judicial Branch of the Federation must make public any sentence that has produced rulings or that has been executed; the interested parties may object to the publication of their personal information.

### **Article 9**

The information referred to in Article 7 must be made available to the public by remote and local electronic means. The subjects compelled by the Law must place computer equipment at the disposal of interested persons so that they may obtain information directly or by printing it out. They must also give support to users who need it and lend every type of assistance possible with regard to the procedures and services they are providing.

The agencies and entities must handle the automation, presentation and content of their information, as well as putting it online, in the terms laid out in the Regulations and the guidelines put forth by the Institute.

### **Article 10**

The agencies and entities must make public, either directly or through the Office of the Legal Counsel of the Executive Branch or the Federal Commission for Regulatory Improvement – in the terms established by the Regulations and at least 20 days in advance of the date when they will be published or given to the head of the Executive Branch to sign – the bills and general administrative arrangements to which Article 4 of the Federal Administrative Procedure Law refers, in accordance with that Law, unless, in the judgment of counsel or the Federal Commission for Regulatory Improvement, as the case may be, their publication could compromise the effects the provision is designed to obtain, or in emergency situations.

### **Article 11**

The reports presented by political parties and national political groups to the Federal Electoral Institute, as well as any audits and inspections ordered by the Commission for Auditing the Resources of Parties and Political Groups, should be made public as soon as they are completed.

Any citizen may request from the Federal Electoral Institute information regarding the use of public resources received by the political parties and national political groups.

### **Article 12**

Subjects compelled by the Law must make public all information regarding the amounts and the recipients of any public resources they give out for any reason, as well as the reports recipients give them on the use and destination of said resources.

[...]

## **Chapter III**

### **Classified and confidential information**

#### **Article 13**

Information is categorized as classified if its disclosure could:

- I. Compromise national security, public security or national defense;

## **Access to Information and Security Sector Governance**

- II. Impair ongoing negotiations or international relations, including that information which other states or international organisms give as confidential to the Mexican State;
- III. Harm the country's financial, economic or monetary stability;
- IV. Put the life, security or health of any person at risk, or
- V. Severely prejudice the verification of observance of the laws, the prevention or prosecution of crimes, the imparting of justice, the collection of taxes, immigration control operations, or procedural strategies in judicial or administrative processes that are ongoing.

### **Article 14**

The following will also be considered exempted information:

- I. That which by any Law's express disposition is considered confidential, classified, commercial classified or government confidential;
- II. Commercial, industrial, tax, bank, and fiduciary secrets, or others so considered in legal provisions;
- III. Prior investigations;
- IV. Judicial files or administrative procedures that have taken the form of a trial, when there has been no ruling;
- V. Liability proceedings against public servants, when an administrative ruling or a definitive jurisdictional ruling has not been made, or
- VI. That which contains the opinions, recommendations or points of view that are part of a public servant's deliberative process, until that time when a final decision is adopted, which itself must be documented.

When the period of classification is over or the causes that gave rise to the classification of the information, referred to in clauses III and IV of this Article, no longer exist, said information may be made public, with the exception of whatever confidential information it may contain.

Information may not be classified when the investigation of grave violations of fundamental rights or crimes against humanity is at stake.

### **Article 15**

Information categorized as classified according to Articles 13 and 14 may retain this categorization for a period of up to twelve years. This information may be declassified when the causes which gave rise to its classification no longer exist, or when the period of classification is over. The availability of this information will be without prejudice to what other laws may establish in this respect.

The Institute, in conformity with the Regulations or the equivalent instance as referred to in Article 61, will establish the criteria for the classification and declassification of information.

Exceptionally, subjects compelled by the Law may request the Institute or the instance established according to Article 61, whichever applies, to extend the period of classification, as long as the causes that gave rise to its classification persist.

### **Article 16**

The heads of the administrative units will be responsible for classifying information according to the criteria established in this Law, its Regulations and the guidelines established by the Institute or the equivalent instance referred to in Article 61, whichever applies.

### **Article 17**

Every semester, the administrative units will produce an index of the files they have identified as classified, organized by subject headings. This index must indicate the administrative unit that generated the information, the date of its classification, the reason, the length of time it will be classified and, when relevant, which parts of the documents are classified. In no instance shall the index itself be considered classified information. The head of each agency or entity must take the necessary measures to ensure the custody and preservation of the classified files. 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.

### **Article 18**

The following will be considered confidential information:

- I. That which private individuals have turned over to the subjects compelled by the Law under this title, in accordance with Article 19, and
- II. Personal information that requires an individual's consent before being disclosed, distributed or commercialized as stipulated in this Law. Information found in public records or in sources to which the public has access will not be considered confidential.

**Article 19**

When private individuals turn over information referred to in division I of the preceding Article to subjects compelled by the Law, the former must indicate which documents contain confidential, classified or commercial classified information, as long as they have the right to classify information according to the applicable provisions. When a request for access that includes confidential information is made, the subjects compelled by the Law will disclose it only with the express consent of the individual to whom that confidential information belongs.

[...]

# **Switzerland: Federal Act on the Principle of Freedom of Information in Public Administration (2007)<sup>10</sup>**

*The Federal Assembly of the Swiss  
Confederation,*

on the basis of Article 173(2) of the Constitution,  
upon consideration of the accompanying Report  
of the Federal Council of 12 February 2003

*decrees as follows:*

## **Section 1 General Provisions**

### **Art. 1 Object and Purpose**

This Act seeks to promote transparency with regard to the mandate, organisation and activities of the Public Administration. For this purpose, it shall contribute to informing the public by ensuring access to official documents.

### **Art. 2 Scope: Ratione Personae**

1. This Act shall apply to:
  - a. The Federal Administration
  - b. Public and private bodies, existing outside of the Federal Administration, insofar as they pass acts or hand down decisions in the first instance within the meaning of Article 5 of the Federal Act of December 20, 1968 on Administrative Procedures (Administrative Procedures Act);<sup>3</sup>
  - c. The Parliamentary Services.
2. This Act shall not apply to the Swiss National Bank or the Swiss Federal Banking Commission.
3. The Federal Council shall be authorised to exclude other departments of the Federal

Administration, as well as other public and private bodies outside the Federal Administration, from the scope of this Act, should:

- a. the functions assigned to same so require;
- b. their competitiveness be prejudiced by being subject to this Act; or
- c. the functions assigned to them be of only minor importance.

### **Art. 3 Scope: Ratione Materiae**

1. This Act shall not apply to:
  - a. Access to official documents relating to:
    1. Civil proceedings;
    2. Criminal proceedings;
    3. International legal and administrative assistance proceedings;
    4. International dispute settlement proceedings;
    5. Constitutional and administrative judiciary proceedings; or
    6. Arbitration proceedings; and
  - b. The consultation, by a party, of the case file in first-instance administrative proceedings.
2. Access to official documents containing personal information about the applicant shall be governed by the Federal Act of 19 June 1992 on Data Protection (Data Protection Act).

<sup>10</sup> Source:<http://www.edoeb.admin.ch/org/00828/index.html?lang=en>

#### **Art. 4 Reservation of Special Provisions**

Special provisions contained in other Federal Acts shall be reserved where they:

- a. declare certain information secret; or
- b. declare certain information accessible subject to requirements differing from those set out herein;

#### **Art. 5 Official Documents**

1. An official document shall be any information:
  - a. which has been recorded, regardless of the medium;
  - b. retained by the authority which issued same or to which it has been communicated; and
  - c. which concern the execution of a public function.
2. Documents which have been produced by means of a simple computerized process from recorded information which meets the requirements pursuant to (a), (b) and (c) above, shall be deemed to be official documents.
3. Not deemed to be official documents are any documents which:
  - a. are used by an authority in a commercial capacity;
  - b. have not been issued; or
  - c. care intended for personal use.

## **Section 2 Right of Access to Official Documents**

#### **Art. 6 Principle of Freedom of Information**

1. Every person shall have the right to inspect official documents and to obtain information about the contents of official documents.
2. The documents may be inspected in situ or a copy thereof may be requested. Legislation governing copyright shall be reserved.

3. Where an official document has already been published by the Federal Government, in paper or electronic format, the provisions pursuant to (1) and (2) above shall be deemed to have been fulfilled.

#### **Art. 7 Exceptions**

1. The right of access shall be limited, deferred or denied, should such access to an official document:
  - a. significantly impair the free opinion-forming and decision-making processes of an authority which is subject to this Act, or of another legislative, administrative or judicial body;
  - b. affect the execution of specific measures taken by an authority in conformity with its objectives;
  - c. be likely to compromise the domestic and international security of Switzerland;
  - d. be likely to affect the interests of Switzerland in matters of foreign policy and international relations;
  - e. be likely to affect relations between the Federal Government and the cantons or inter-cantonal relations;
  - f. be likely to affect the economic or monetary interests of Switzerland;
  - g. reveal professional, business or manufacturing secrets; or
  - h. result in the release of information provided voluntarily by a third party to an authority which undertook to maintain secrecy with regard thereto.
2. The official document prejudice the privacy of a third party, unless exceptionally outweighed by public interest.

#### **Art. 8 Special Cases**

1. There shall be no right of access to official documents of joint reporting proceedings.
2. Access to official documents shall only be granted after the political or administrative

## **Access to Information and Security Sector Governance**

- decisions which they form the basis of have been taken.
3. By way of exception, the Federal Council may decide to withhold access to official documents resulting from official departmental consultation processes even after rulings have been made.
  4. Under no circumstances shall access to official documents about the status of pending or future negotiations be granted.
  5. Access to reports on the evaluation of the performance of the Federal Administration and the effectiveness of its measures shall be ensured.

### **Art. 9 Protection of Personal Data**

1. Official documents containing personal data shall, wherever possible, be rendered anonymous prior to inspection.
2. Where a request for access covers official documents which cannot be rendered anonymous, Article 19 of the Federal Data Protection Act shall apply. The relevant procedure shall be governed by this Act.

## **Section 3 Procedure for Access to Official Documents**

### **Art. 10 Access Application**

1. An application for access to official documents shall be addressed to the authority which created same or received same as primary addressee from third parties not subject to this Act.
2. The Federal Council may provide a special procedure for access to official documents by Swiss representation abroad and by missions to international organisations.
3. The application must be formulated in a sufficiently accurate manner.
4. The Federal Council shall enact regulations governing the particulars of this procedure:
  - a. it shall take the special needs of the media into account;

- b. should a large number of applications cover the same documents, it may stipulate other modalities governing such access;
- c. it may extend the processing deadlines for applications which require particularly extensive processing.

### **Art. 11 Consultation**

1. Should an application be made for access to official documents which contain personal data, and which the authority is considering granting, it shall consult the person concerned and afford him the opportunity to submit comments within ten days.
2. The authority shall then inform such consulted person of the position it intends to take concerning the application for access.

### **Art. 12 Decision of the Authority**

1. The authority shall make a decision as soon as possible; no later than 20 days after receipt of the application.
2. Said deadline may, under exceptional circumstances, be extended by 20 days, should the application for access concern a large number of documents or documents which are complex or difficult to obtain. Should an application concern official documents containing personal information, the deadline shall be extended for the required period.
3. Should an application concern official documents containing personal information, the authority shall suspend access until the legal situation has been clarified.
4. The authority shall inform the applicant, with summary grounds, of any extension of the deadline, limitation or denial of access. Information concerning the limitation or denial of access, as well as the grounds therefore, shall be conveyed in writing.

### **Art. 13 Mediation**

1. A request for mediation may be filed by any person:

- a. whose access to official documents has been limited, deferred or denied;
  - b. whose application was not decided by the authority within the deadline;
  - c. who was consulted pursuant to Art. 11, should the authority intend granting access contrary to his disapproval.
2. The request for mediation must be filed in writing with the Federal Data Protection and Information Commissioner within 20 days of receipt of the decision from the authority or the date of the authority's failure to comply with the deadline.
  3. Should mediation succeed, the matter shall be deemed to have been settled.

#### **Art. 14 Recommendation**

Should mediation fail to succeed, the Federal Data Protection and Information Commissioner shall provide the participants to the mediation proceedings with a written recommendation within 30 days of receipt of the request for mediation.

#### **Art. 15 Decision**

1. Within ten days of receipt of the recommendation, the applicant or the person consulted may request a decision pursuant to Article 5 of the Administrative Procedures Act.
2. Furthermore, the authority shall hand down a decision, where, contrary to the recommendation, it intends to:
  - a. limit, defer or deny the right of access to an official document;
  - b. grant the right of access to an official document containing personal information.
3. A decision shall be handed down within 20 days of the date of receipt of the recommendation or the request for a decision pursuant to (1) above.

#### **Art. 16 Appeal**

1. Appeals proceedings shall be subject to the general provisions found in the

relevant legislation governing the Federal administration of justice.

2. The instances called upon to hear any appeals shall also have access to official documents which are secret.

#### **Art. 17 Fees**

1. In principle, access to official documents shall be subject to payment of a fee.
2. No fee shall be charged for:
  - a. the processing of an application which gives rise to minimal costs;
  - b. mediation proceedings (Art. 13); and
  - c. proceedings before the first instance (Art. 15).
3. The Federal Council shall enact modalities and fee rates on the basis of the effective costs incurred. Special provisions set out in other legislative Acts shall be reserved.
4. Fees may, in any event, be charged for the release of reports, brochures and other printed material and information carriers.

### **Section 4 Federal Data Protection and Information Commissioner**

#### **Art. 18 Duties and Competencies**

The Federal Data Protection and Information Commissioner (the Commissioner) pursuant to Article 26 of the Federal Data Protection Act shall, in particular, have the following duties and competencies under the present Act:

- a. Conducting mediation proceedings (Art. 13) and making a recommendation (Art. 14), should mediation not succeed;
- b. Providing information ex officio, or at the request of individuals or authorities, on the modalities governing access to official documents;
- c. Commenting on draft legislation and measures of the Federal Government

## **Access to Information and Security Sector Governance**

which have a fundamental impact on the principle of freedom of information.

### **Art. 19 Evaluation**

1. The Commissioner shall review the execution and effectiveness of this Act and, in particular, the costs incurred by its implementation, and shall report on a regular basis to the Federal Council.
2. The Commissioner shall submit the first report on the implementation costs of this Act to the Federal Council within three years of its entry into force.
3. The reports of the Commissioner shall be published.

### **Art. 20 Right to Information and Inspection**

1. Within the context of mediation proceedings, the Commissioner shall have access to official documents, even if same are subject to secrecy.
2. The Commissioner and his secretariat shall be subject to official secrecy to the same extent as the authorities whose official documents they inspect or from whom they obtain information.

## **Section 5 Concluding Provisions**

### **Art. 21 Execution**

The Federal Council may, in particular, enact provisions governing the:

- a. Processing of official documents;
- b. Information pertaining to official documents;
- c. Publication of official documents.

### **Art. 22 Amendments to Existing Legislation**

Amendments to existing legislation shall be governed pursuant to the Annex.

### **Art. 23 Transitional Provisions**

This Act shall apply to official documents produced or received by authorities after its entry into force.

### **Art. 24 Referendum and Entry into Force**

1. This Act shall be subject to optional referendum.
2. The Federal Council shall determine the date of entry into force.

Date of entry into force: 1 July 2006.

# Palestinian National Authority: Draft Law on the Right to Access Information (2005)<sup>11</sup>

**In the Name of God, the Most Gracious, the Most Merciful**

## Chapter I

### General Provisions

#### Article 1

For the purposes of the enforcement of the provisions of this Law, the following words and expressions shall have the meanings designated thereto below unless the context determines otherwise:

**The Authority:** The Palestinian National Authority.

**The Commissioner General of Information:** The Commissioner General of Information.

**The Office:** The Office of the Commissioner General of Information.

**The public institution:** All Ministries, departments, agencies, legislative, judicial and executive authorities, local bodies, and private institutions which manage a public facility or perform public works or possess information pertaining to the environment or public health and safety, or any other institution which the Commissioner General deems to be a public institution for the purposes of the enforcement of this Law.

**The competent functionary:** The functionary who is appointed by the public institution to view the requests to access information.

**The piece of information:** The piece of information which is available in any of the registers and written or electronically-saved documents, or drawings, maps, tables, pictures, films, microfilms, sound recordings, video tapes, charts, or any data read with special devices, or any other forms which the Commissioner General deems that they fall under the scope of the piece of information in accordance with this Law.

**The alternative formula:** The formula which enables the persons with special needs to view the required piece of information.

#### Article 2

This Law shall aim to:

1. Enable the citizen and resident in Palestine to exercise the right to access information which is available at the public institutions in accordance with the provisions of this Law.
2. Promote the spirit of transparency and accountability at the Palestinian public institutions and encourage openness with the people.

<sup>11</sup> This Draft Law was submitted to the PLC plenary in 2005 but was never adopted.

## **Access to Information and Security Sector Governance**

### **Article 3**

All information which is in the possession of public institutions shall be deemed to be subject to be accessed, except for those which fall within the scope of the exceptions set forth in this Law.

### **Article 4**

The public institution must appoint a competent functionary to examine the requests to access information and shall grant him or her the powers necessary to search for and access the requested piece of information.

### **Article 5**

Public institutions must keep the information which is in their possession in a regulated manner and in an arrangement which makes it easy for the competent functionary to extract it. Public institutions must also keep the information electronically when possible.

### **Article 6**

Public institutions must organise training courses for their functionaries that are related to the importance of the right to access [information] and enable the citizen to exercise it, along with the manner of the keeping of information and the best and fastest methods to extract them.

## **Chapter Two**

### **Principles of the Right of Access Obligation of Publication**

#### **Article 7**

Public institutions must publish annual reports entailing at least:

1. Administrative information about the mechanism of the function of the public institution, to include the costs, objectives, audited accounts, rules and accomplishments.
2. The procedures on the basis of which the individuals can be familiar with the public policy and projects of the public institution.

3. The types of information which the public institution keeps and the circumstances under which it is kept.
4. The content of any decision or policy that may affect the people and the reasons behind the taking of the decision and the objectives anticipated therefrom.
5. Any other information which the Commissioner General deems to be necessary to be published.

### **Article 8**

The industrial institution, both public and private, must publish semi-annual reports in which they state at least the following information:

1. The locations of the utilised toxic materials as well as their nature and risks.
2. The quantity of the discharges resulting from manufacturing.
3. The manner of the disposal of wastes.

The Opening of Public Meetings to the Public

### **Article 9**

Each public institution, which intends to hold a public meeting, must announce the date and venue of such meeting and the objective therefrom. The public may not be prohibited from attending such meeting except in accordance with the exceptions set forth in this Law.

### **Protection of the Informant**

#### **Article 10**

No penalty may be imposed upon the functionary who reveals information about contraventions or violations that are perpetrated against the Law.

## **Chapter Three**

### **The Request to Access Information**

#### **Article 11**

The request to access information shall be submitted in writing to the institution which possesses the piece of information. Such request must include sufficient details that enable the competent functionary to extract the piece of information with minimum effort.

#### **Article 12**

The competent functionary, immediately after he or she receives the request, give a notice to the person submitting the request, in which he or she states the date on which the request has been submitted, the type of the requested piece of information and the period of time required for responding to the request.

#### **Article 13**

The competent functionary must respond to the request within 15 days from the date on which it was submitted. The competent functionary may extend such period once for a period of time not exceeding 15 days in the event the request entails a large number of pieces of information, or because the accessing of the piece of information requires the consulting with a third party or another public institution. Non-response within that period shall be deemed to be a rejection of the request.

#### **Article 14**

In case the request is approved, the competent functionary must enable the person submitting the request to access the information which he or she detailed in the request and define for him or her the cost associated with the accessing of the required piece of information. In the event the request includes more than one piece of information, the competent functionary may allow the person submitting the request to view a portion of the information if the other information fall within the scope of exceptions defined in this Law.

#### **Article 15**

Upon approval of the request, the competent functionary must present the piece of information to the person submitting the

request in accordance with the formula which is available at the public institutions. The functionary may not only inform the person submitting the request with the piece of information verbally without presenting to him or her the document containing such piece of information. The instructions to be issued forth by the Commissioner General shall define the manner by which the person submitting the request can obtain copies of the required information.

#### **Article 16**

In case the person submitting the request is with special needs, the competent functionary must present the piece of information with an alternative formula that is suitable to the disability of the person submitting the request, if such formula is available at the institution. The competent functionary may convert the piece of information into an alternative formula in case he or she deems it necessary. He or she must conduct the conversion in the event the person submitting the request accepts that the conversion is conducted at his or her own expense.

#### **Article 17**

The competent functionary may refer the request to another institution, after having notified the person submitting the request thereof, in case he or she finds that the relation of such institution to the piece of information is closer. This covers the fact that the other institution has prepared the piece of information or that it possesses alternative formulas of the piece of information. In such case, the request shall be deemed as if having been submitted to the public institution to which the request has been referred.

#### **Article 18**

In the event the request is rejected, the competent functionary must state in a written response which he or she shall hand to the person submitting the request the reason behind the rejection of the request. The reason may not be beyond [the following]:

1. That the piece of information is not in the possession of the institution.
2. That the required piece of information falls within the scope of the exceptions set forth in this Law.

## **Chapter Four**

### **The Exceptions**

#### **National Security and Public Order**

##### **Article 19**

The competent functionary must refuse to reveal any piece of information in the event such revealing is proved to cause damage to the defence capabilities and national security of the state. This includes:

1. Weapons, tactics, strategies and military forces as well as the military operations which aim to protect the homeland.
2. The intelligence information which pertains to the blocking of aggressive acts and crimes perpetrated against the internal and external security of the state in pursuance of the Laws in force.
3. The international communications and correspondences which are related to the defence affairs and military alliances.
4. Any piece of information which the Commissioner General is convinced that it causes damage to the public security and order.

##### **Article 20**

The competent functionary must refuse to reveal any piece of information that is related to a state or international organisation with which it has been agreed to keep such piece of information classified.

##### **Article 21**

The competent functionary may not refuse to disclose information in the cases mentioned under Articles (19 and 20) above in the event such information is still in the possession of the institution and date back to more than twenty years, except in cases in which the Commissioner General is convinced of the necessity to keep such information classified for another renewable period of time.

##### **Article 22**

The competent functionary at the institutions which assume the task of investigation in crimes and control of contraventions and performance of Police functions shall be entitled to refuse to disclose information in the event such disclosure causes damage to the investigations and implementation of required tasks, or in the event such disclosure jeopardises the reputation of persons whose conviction is not proved yet.

#### **Issues of Economic Security**

##### **Article 23**

The competent functionary may refuse to reveal any piece of information containing:

1. Professional or commercial secrets that pertain to the institution.
2. Secrets the revealing of which leads to causing material damages to the economic interests of the state or its ability to manage the national economy, or results in personal gains for a person or body. This includes:
  - A. The prices of the currency in circulation in Palestine.
  - B. The anticipated changes in the fees of the customs tariff, taxes, fees and any other sources of revenues.
  - C. The anticipated changes in the rates of interest related to governmental loans.
  - D. The anticipated changes in the prices of governmental properties, including shares, movable properties and real estate.
  - E. Transactions which the public institution intends to conclude in regard of a merchandise, the revealing of which may lead to the influencing of the prices of such merchandise in the market.

##### **Article 24 Commercial Secrets**

The competent functionary must refuse to disclose any piece of information that feature professional secrets of a third party, or the

disclosing of which leads to the weakening of the competitive status of a third party unless the third party agrees to the disclosure.

#### **Article 25      The Internal Affairs of the Institution**

The competent functionary may refuse to disclose the piece of information in the event it is related to the internal affairs of the institution and its functionaries as well as the internal orders, discussions and preliminary proposals.

#### **Article 26    Public Health and Safety**

The competent functionary may refuse to disclose the piece of information in the event it pertains to unconfirmed anticipations about natural disasters or epidemic diseases the possibility for the occurrence of which is weak.

#### **Article 27**

The competent functionary may refuse to reveal any piece of information the revealing of which may harm or cause damage to the safety of individuals.

#### **Article 28   Privacy**

The competent functionary must refuse to disclose any piece of information that pertains to a third party and which is related to his or her private life except in the following cases:

1. If the concerned person agrees to such disclosure.
2. If such piece of information is publicly disseminated.
3. If such disclosure has been requested by a judicial judgement or under an approval from the Commissioner General.
4. If the person submitting the request is a custodian of the third party.
5. If the person submitting the request is a relative to the third party and submits the request following his or her death by at least twenty years.

## **Chapter Five**

### **The Commissioner General of Information**

#### **Article 29**

In pursuance of the provisions of this Law, an office for the Commissioner General of Information shall be established. It shall enjoy the judicial character and the independence necessary to exercise its functions. The Office shall be allocated a special budget within the public budget of the Palestinian National Authority.

#### **Article 30**

The Office shall be deemed to an authority of appeal for each person whose request to access information has been rejected. The Office shall aim to the ensuring of the enforcement of the provisions of this Law and accomplish the goals anticipated therefrom. Thus, it shall be entitled to exercise the following powers:

1. Put forward, regulate and implement the programmes, plans and policies pertaining to the defence of the right of the individual to access and view information.
2. Educate and raise awareness of the citizen about the importance of the right of access and the positive results of the exercising of it on the level of the individual, the society and the state.
3. Contribute to the training of functionaries and officials at the public institutions on the manner and significance of the enabling of individuals to access information.
4. Monitor the contraventions and publish the reports and studies which entail the impediments to the exercise of the right of access and how to overcome them.

#### **Article 31**

The main headquarters of the Office shall be in Jerusalem. It may establish branches throughout governorates.

#### **Article 32**

The Office shall be deemed to an authority of appeal for each person:

## **Access to Information and Security Sector Governance**

1. whose request to access information has been rejected;
2. on whose request high charges have been imposed;
3. whose request to access the piece of information in an alternative formula has been rejected;
4. the period of time required to respond to his or her request has been extended in a manner contravening the provisions of Article (13) above;
5. whose request has been referred to more than one institution without approval thereof; and
6. any other cases which the Commissioner General of Information admits.

### **Article 33**

The appeal must be submitted to the Office within 30 days from the date on which the request was rejected, or from the date on which the institution took the measure which the person submitting the request wishes to appeal.

### **Article 34**

The Office must respond to the appeal within a period of time not exceeding three months from the date on which it was submitted thereto. The Office must, immediately after it receives and admits the appeal, send a letter to the competent functionary at the institution which rejected the request to access information, in which it notifies him or her of the appeal and requires that the reasons behind rejection be made clear.

### **Article 35**

The Commissioner General of Information shall preside over the Office. He or she shall be appointed by a decision from the Council of Ministers and approval of the Palestinian Legislative Council for a period of four years that is renewable for one time only. His or her salary and other financial entitlements shall be defined in the decision.

### **Article 36**

The Commissioner General shall be responsible for the following up with and issuing forth of the decisions pertaining to

the appeals to the Office, the appointing of functionaries at the Office and setting forth of a regulation thereto.

### **Article 37**

The Commissioner General of Information must be devoted to his or her work at the Office. He or she may not, during the assumption of his or her function, perform any work or occupy any position or function with or without pay.

### **Article 38**

The services of the Commissioner shall, legally, expire in the following cases:

1. In case he or she is convicted with a crime or misdemeanour which involves moral or trust turpitude.
2. In case he or she exercises the acts of any other function or position.
3. In case he or she is confined or he or she is declared bankrupt.

### **Article 39**

The recommendations issued forth by the Commissioner General shall be deemed to be binding to all public institutions.

### **Article 40**

For the purposes of the implementation by the Commissioner General of his or her tasks, the following powers shall be bestowed upon him or her:

1. The right to enter any public institution and inspect its registers and papers and any documents that are connected to the required information.
2. Investigate any functionary in private in order to access the required information.
3. Refer to the judiciary the persons responsible for the concealing or damaging of the information or modifying it in a manner that contravenes its truth with the intention to evade from presenting it.
4. Inquire the senior state officials such as Ministers and those alike about the reason behind their concealing of the information in the event such concealing is resultant

from orders issued forth by them directly. The Commissioner General, in this case and as he or she is not convinced of the submitted justifications, shall be entitled to submit an immediate report to the President of the Authority or the Chairman of the Council of Ministers or the Legislative Council to take the appropriate measures.

#### **Article 41**

The Commissioner General shall adhere to the submitting of regular reports every six months to each one of: the President of the National Authority, the Chairman of the Council of Ministers and the Palestinian Legislative Council. The reports must entail the following:

1. The cases of unjustified abstention from the submitting of information.
2. The executive problems which he or she faces during the implementation of his or her tasks.
3. Any other recommendations which the Commissioner deems fit.

## **Chapter Six**

### **The Fees**

#### **Article 42**

The fees associated with the requests to access information shall be defined in a bylaw to be developed by the Commissioner General and issued forth by the Council of Ministers. The fee must not exceed ten Jordanian Dinars or its equivalent of the currency in circulation, with the exception of the following cases:

1. The covering of the cost of photocopying or required copies as per their market value.
2. The covering of the alternative formulas of the information as per their market value.
3. In the event the request incorporates more than one piece of information.

#### **Article 43**

The fees associated with the appeal must not exceed ten Jordanian Dinars or its equivalent of the currency in circulation.

## **Chapter Seven**

### **Conclusive Provisions**

#### **Article 44**

Each provision which contradicts the provisions of this Law shall be repealed.

#### **Article 45**

The Council of Ministers must issue forth the bylaws necessary for the enforcement of this Law within a period of time not exceeding six months from the date on which it is published.

#### **Article 46**

All competent authorities – each one within its sphere of jurisdiction – shall implement the provisions of this Law which shall enter into force one year following its publication.



# **Part II**

# **Standards Promoted by Regional and International Bodies**

# Commonwealth Freedom of Information Principles (1999)<sup>12</sup>

Trinidad and Tobago, 1999

## Annex 1

1. Member countries should be encouraged to regard freedom of information as a legal and enforceable right.
2. There should be a presumption in favour of disclosure and Governments should promote a culture of openness.
3. The right of access to information may be subject to limited exemptions but these should be narrowly drawn.
4. Governments should maintain and preserve records.
5. In principle, decisions to refuse access to records and information should be subject to independent review.

---

<sup>12</sup> Annex 1 of the Communiqué of the Meeting of Commonwealth Law Ministers, Port of Spain, Trinidad and Tobago, 3-7 May 1999, available at: <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-65439>

# Council of Europe Convention on Access to Official Documents (2009)<sup>13</sup>

Tromsø, 18.6.2009

## Preamble

The member States of the Council of Europe and the other signatories hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members for the purpose of safeguarding and realising the ideals and principles which are their common heritage;

Bearing in mind, in particular, Article 19 of the Universal Declaration of Human Rights, Articles 6, 8 and 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms, the United Nations Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters (Aarhus, 25 June 1998) and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (ETS No. 108);

Bearing in mind also the Declaration of the Committee of Ministers of the Council of Europe on the freedom of expression and information, adopted on 29 April 1982, as well as recommendations of the Committee of Ministers to member States No. R (81) 19 on the access to information held by public authorities, No. R (91) 10 on the communication to third parties of personal data held by public bodies, No. R (97) 18 concerning the protection of personal data collected and processed for statistical purposes, No. R (2000) 13 on a European policy on access to archives and Rec(2002)2 on access to official documents;

Considering the importance in a pluralistic, democratic society of transparency of public authorities;

Considering that exercise of a right to access to official documents:

- i. provides a source of information for the public;
- i.i helps the public to form an opinion on the state of society and on public authorities;
- iii. fosters the integrity, efficiency, effectiveness and accountability of public authorities, so helping affirm their legitimacy;

Considering, therefore, that all official documents are in principle public and can be withheld subject only to the protection of other rights and legitimate interests,

Have agreed as follows:

## Section I

### Article 1 – General provisions

1. The principles set out hereafter should be understood without prejudice to those domestic laws and regulations and to international treaties which recognise a wider right of access to official documents.
2. For the purposes of this Convention:
  - a. (i) “public authorities” means:
    1. government and administration at national, regional and local level;

<sup>13</sup> <https://wcd.coe.int/wcd/ViewDoc.jsp?id=1377737&Site=CM>

## **Access to Information and Security Sector Governance**

2. legislative bodies and judicial authorities insofar as they perform administrative functions according to national law;
  3. natural or legal persons insofar as they exercise administrative authority.
- (ii) Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, by a declaration addressed to the Secretary General of the Council of Europe, declare that the definition of "public authorities" also includes one or more of the following:
1. legislative bodies as regards their other activities;
  2. judicial authorities as regards their other activities;
  3. natural or legal persons insofar as they perform public functions or operate with public funds, according to national law.
- b. "official documents" means all information recorded in any form, drawn up or received and held by public authorities.
- 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.

### **Article 2 – Right of access to official documents**

1. Each Party shall guarantee the right of everyone, without discrimination on any ground, to have access, on request, to official documents held by public authorities.
2. Each Party shall take the necessary measures in its domestic law to give effect to the provisions for access to official documents set out in this Convention.
3. These measures shall be taken at the latest at the time of entry into force of this Convention in respect of that Party.

### **Article 3 – Possible limitations to access to official documents**

1. Each Party may limit the right of access to official documents. Limitations shall be

Concerned States may, at the time of signature or when depositing their instrument of ratification, acceptance, approval or accession, by a declaration addressed to the Secretary General of the Council of Europe, declare that communication with the reigning Family and its Household or the Head of State shall also be included among the possible limitations.

2. Access to information contained in an official document may be refused if its disclosure would or would be likely to harm any of the interests mentioned in paragraph 1, unless there is an overriding public interest in disclosure.
3. The Parties shall consider setting time limits beyond which the limitations mentioned in paragraph 1 would no longer apply.

**Article 4 – Requests for access to official documents**

1. An applicant for an official document shall not be obliged to give reasons for having access to the official document.
2. Parties may give applicants the right to remain anonymous except when disclosure of identity is essential in order to process the request.
3. Formalities for requests shall not exceed what is essential in order to process the request.

**Article 5 – Processing of requests for access to official documents**

1. The public authority shall help the applicant, as far as reasonably possible, to identify the requested official document.
2. A request for access to an official document shall be dealt with by any public authority holding the document. If the public authority does not hold the requested official document or if it is not authorised to process that request, it shall, wherever possible, refer the application or the applicant to the competent public authority.
3. Requests for access to official documents shall be dealt with on an equal basis.
4. A request for access to an official document shall be dealt with promptly. The decision shall be reached, communicated and executed as soon as possible or within a reasonable time limit which has been specified beforehand.
5. A request for access to an official document may be refused:
  - i. if, despite the assistance from the public authority, the request remains too vague to allow the official document to be identified; or
  - ii. if the request is manifestly unreasonable.
6. A public authority refusing access to an official document wholly or in part shall give the reasons for the refusal. The applicant has the right to receive on request a written

justification from this public authority for the refusal.

**Article 6 – Forms of access to official documents**

1. When access to an official document is granted, the applicant has the right to choose whether to inspect the original or a copy, or to receive a copy of it in any available form or format of his or her choice unless the preference expressed is unreasonable.
2. If a limitation applies to some of the information in an official document, the public authority should nevertheless grant access to the remainder of the information it contains. Any omissions should be clearly indicated. However, if the partial version of the document is misleading or meaningless, or if it poses a manifestly unreasonable burden for the authority to release the remainder of the document, such access may be refused.
3. The public authority may give access to an official document by referring the applicant to easily accessible alternative sources.

**Article 7 – Charges for access to official documents**

1. Inspection of official documents on the premises of a public authority shall be free of charge. This does not prevent Parties from laying down charges for services in this respect provided by archives and museums.
2. A fee may be charged to the applicant for a copy of the official document, which should be reasonable and not exceed the actual costs of reproduction and delivery of the document. Tariffs of charges shall be published.

**Article 8 – Review procedure**

1. An applicant whose request for an official document has been denied, expressly or impliedly, whether in part or in full, shall have access to a review procedure before a court or another independent and impartial body established by law.
2. An applicant shall always have access to an expeditious and inexpensive review

## **Access to Information and Security Sector Governance**

procedure, involving either reconsideration by a public authority or review in accordance with paragraph 1.

### **Article 9 – Complementary measures**

The Parties shall inform the public about its right of access to official documents and how that right may be exercised. They shall also take appropriate measures to:

- a. educate public authorities in their duties and obligations with respect to the implementation of this right;
- b. provide information on the matters or activities for which they are responsible;
- c. manage their documents efficiently so that they are easily accessible;
- d. apply clear and established rules for the preservation and destruction of their documents.

### **Article 10 – Documents made public at the initiative of the public authorities**

At its own initiative and where appropriate, a public authority shall take the necessary measures to make public official documents which it holds in the interest of promoting the transparency and efficiency of public administration and to encourage informed participation by the public in matters of general interest.

## **Section II**

### **Article 11 – Group of Specialists on Access to Official Documents**

1. A Group of Specialists on Access to Official Documents shall meet at least once a year with a view to monitoring the implementation of this Convention by the Parties, notably:
  - a. reporting on the adequacy of the measures in law and practice taken by the Parties to give effect to the provisions set out in this Convention;

- b.
  - i. expressing opinions on any question concerning the application of this Convention;
  - ii. making proposals to facilitate or improve the effective use and implementation of this Convention, including the identification of any problems;
  - iii. exchanging information and reporting on significant legal, policy or technological developments;
  - iv. making proposals to the Consultation of Parties for the amendment of this Convention;
  - v. formulating its opinion on any proposal for the amendment of this Convention made in accordance with Article 19.

2. The Group of Specialists may request information and opinions from civil society.
3. The Group of Specialists shall consist of a minimum of 10 and a maximum of 15 members. The members are elected by the Consultation of Parties for a period of four years, renewable once, from a list of experts, each Party proposing two experts. They shall be chosen from among persons of the highest integrity recognised for their competence in the field of access to official documents. A maximum of one member may be elected from the list proposed by each Party.
4. The members of the Group of Specialists shall sit in their individual capacity, be independent and impartial in the exercise of their functions and shall not receive any instructions from governments.
5. The election procedure of the members of the Group of Specialists shall be determined by the Committee of Ministers, after consulting with and obtaining the unanimous consent of the Parties to the Convention, within a period of one

year following the entry into force of this Convention. The Group of Specialists shall adopt its own rules of procedure.

#### **Article 12 – Consultation of the Parties**

1. The Consultation of the Parties shall be composed of one representative per Party.
2. The Consultation of the Parties shall take place with a view to:
  - a. considering the reports, opinions and proposals of the Group of Specialists;
  - b. making proposals and recommendations to the Parties;
  - c. making proposals for the amendment of this Convention in accordance with Article 19;
  - d. formulating its opinion on any proposal for the amendment of this Convention made in accordance with Article 19.
3. The Consultation of the Parties shall be convened by the Secretary General of the Council of Europe within one year after the entry into force of this Convention in order to elect the members of the Group of Specialists. It shall subsequently meet at least once every 4 years and in any case, when the majority of the Parties, the Committee of Ministers or the Secretary General of the Council of Europe requests its convocation. The Consultation of the Parties shall adopt its own rules of procedure.
4. After each meeting, the Consultation of the Parties shall submit to the Committee of Ministers an activity report.

#### **Article 13 – Secretariat**

The Consultation of the Parties and the Group of Specialists shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this Section.

#### **Article 14 – Reporting**

1. Within a period of one year following the entry into force of this Convention in respect of a Contracting Party, the latter

shall transmit to the Group of Specialists a report containing full information on the legislative and other measures taken to give effect to the provisions of this Convention.

2. Thereafter, each Party shall transmit to the Group of Specialists before each meeting of the Consultation of the Parties an update of the information mentioned in paragraph 1.
3. Each Party shall also transmit to the Group of Specialists any information that it requests to fulfil its tasks.

#### **Article 15 – Publication**

The reports submitted by Parties to the Group of Specialists, the reports, proposals and opinions of the Group of Specialists and the activity reports of the Consultation of the Parties shall be made public.

### **Section III**

#### **Article 16 – Signature and entry into force of the Convention**

1. This Convention shall be open for signature by the member States of the Council of Europe.
2. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.
3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which 10 member States of the Council of Europe have expressed their consent to be bound by the Convention in accordance with the provisions of paragraph 2.
4. In respect of any Signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention

## **Access to Information and Security Sector Governance**

in accordance with the provisions of paragraph 2.

### **Article 17 – Accession to the Convention**

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may, after consulting the Parties to this Convention and obtaining their unanimous consent, invite any State which is not a member of the Council of Europe or any international organisation to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by unanimous vote of the representatives of the Parties entitled to sit on the Committee of Ministers.
2. In respect of any State or international organisation acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

### **Article 18 – Territorial application**

1. Any State may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.
2. Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration for whose international relations it is responsible. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.
3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General. The withdrawal

shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

### **Article 19 – Amendments to the Convention**

1. Amendments to this Convention may be proposed by any Party, the Committee of Ministers of the Council of Europe, the Group of Specialists or the Consultation of the Parties.
2. Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the Parties.
3. Any amendment shall be communicated to the Consultation of the Parties, which, after having consulted the Group of Specialists, shall submit to the Committee of Ministers its opinion on the proposed amendment.
4. The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Consultation of the Parties and may approve the amendment.
5. The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 shall be forwarded to the Parties for acceptance.
6. Any amendment approved in accordance with paragraph 4 shall come into force on the first day of the month following the expiration of a period of one month after the date on which all Parties have informed the Secretary General that they have accepted it.

### **Article 20 – Declarations**

Any Party may, at the time of the signature or when depositing its instrument of ratification, acceptance, approval or accession, make one or more of the declarations provided for in Articles 1.2, 3.1 and 18. It shall notify any changes to this information to the Secretary General of the Council of Europe.

### **Article 21 – Denunciation**

1. Any Party may at any time denounce this Convention by means of a notification

addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.

#### **Article 22 – Notification**

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe and any State and international organisation which has acceded or been invited to accede to this Convention of:

- a. any signature;
- b. the deposit of any instrument of ratification, acceptance, approval or accession;
- c. any date of entry into force of this Convention in accordance with Articles 16 and 17;
- d. any declaration made under Articles 1.2, 3.1 and 18;
- e. any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Tromsø, this 18th day of June 2009, in English and French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe and to any State and international organisation invited to accede to this Convention.



# **Part III**

## **Standards Promoted by Non-Governmental Organisations**

# The Johannesburg Principles on National Security, Freedom of Expression and Access to Information (1996)<sup>14</sup>

Johannesburg, November 1996

## Introduction

These Principles were adopted on 1 October 1995 by 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.

The Principles are based on international and regional law and standards relating to the protection of human rights, evolving state practice (as reflected, *inter alia*, in judgments of national courts), and the general principles of law recognized by the community of nations.

These Principles acknowledge the enduring applicability of the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights and the Paris Minimum Standards of Human Rights Norms In a State of Emergency.

## Preamble

The participants involved in drafting the present Principles:

Considering that, in accordance with the principles proclaimed in the Charter of the United Nations, recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world;

Convinced that it is essential, if people are not to be compelled to have recourse, as a last resort, to rebellion against tyranny and oppression, that human rights should be protected by the rule of law;

Reaffirming their belief that freedom of expression and freedom of information are vital to a democratic society and are essential for its progress and welfare and for the enjoyment of other human rights and fundamental freedoms;

Taking into account relevant provisions of the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the UN Convention on the Rights of the Child, the UN Basic Principles on the Independence of the Judiciary, the African Charter on Human and Peoples' Rights, the American Convention on Human Rights and the European Convention on Human Rights;

Keenly aware that some of the most serious violations of human rights and fundamental freedoms are justified by governments as necessary to protect national security;

Bearing in mind that it is imperative, if people are to be able to monitor the conduct of their government and to participate fully in a democratic society, that they have access to government-held information;

Desiring to promote a clear recognition of the limited scope of restrictions on freedom of expression and freedom of information that may be imposed in the interest of national security, so as to discourage governments from using the pretext of national security to place unjustified restrictions on the exercise of these freedoms;

<sup>14</sup> Source: <http://www.article19.org/pdfs/standards/righttoknow.pdf>

Recognizing the necessity for legal protection of these freedoms by the enactment of laws drawn narrowly and with precision, and which ensure the essential requirements of the rule of law; and

Reiterating the need for judicial protection of these freedoms by independent courts;

Agree upon the following Principles, and recommend that appropriate bodies at the national, regional and international levels undertake steps to promote their widespread dissemination, acceptance and implementation:

## **I. GENERAL PRINCIPLES**

### **Principle 1: Freedom of Opinion, Expression and Information**

- (a) Everyone has the right to hold opinions without interference.
- (b) Everyone has the right to freedom of expression, which includes the 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 or her choice.
- (c) The exercise of the rights provided for in paragraph (b) may be subject to restrictions on specific grounds, as established in international law, including for the protection of national security.
- (d) No restriction on freedom of expression or information on the ground of national security may be imposed unless the government can demonstrate that the restriction is prescribed by law and is necessary in a democratic society to protect a legitimate national security interest. The burden of demonstrating the validity of the restriction rests with the government.

### **Principle 1.1: Prescribed by Law**

- (a) Any restriction on expression or information must be prescribed by law. The law must be accessible, unambiguous, drawn narrowly and with precision so as to enable

individuals to foresee whether a particular action is unlawful.

- (b) The law should provide for adequate safeguards against abuse, including prompt, full and effective judicial scrutiny of the validity of the restriction by an independent court or tribunal.

### **Principle 1.2: Protection of a Legitimate National Security Interest**

Any restriction on expression or information that a government seeks to justify on grounds of national security must have the genuine purpose and demonstrable effect of protecting a legitimate national security interest.

### **Principle 1.3: Necessary in a Democratic Society**

To establish that a restriction on freedom of expression or information is necessary to protect a legitimate national security interest, a government must demonstrate that:

- (a) the expression or information at issue poses a serious threat to a legitimate national security interest;
- (b) the restriction imposed is the least restrictive means possible for protecting that interest; and
- (c) the restriction is compatible with democratic principles.

### **Principle 2: Legitimate National Security Interest**

- (a) A restriction sought to be justified on the ground of national security is not legitimate unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government.
- (b) In particular, a restriction sought to be justified on the ground of national security is not legitimate if its genuine purpose or demonstrable effect is to protect interests

## **Access to Information and Security Sector Governance**

unrelated to national security, including, for example, to protect a government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest.

### **Principle 3: States of Emergency**

In time of public emergency which threatens the life of the country and the existence of which is officially and lawfully proclaimed in accordance with both national and international law, a state may impose restrictions on freedom of expression and information but only to the extent strictly required by the exigencies of the situation and only when and for so long as they are not inconsistent with the government's other obligations under international law.

### **Principle 4: Prohibition of Discrimination**

In no case may a restriction on freedom of expression or information, including on the ground of national security, involve discrimination based on race, colour, sex, language, religion, political or other opinion, national or social origin, nationality, property, birth or other status.

## **II. RESTRICTIONS ON FREEDOM OF EXPRESSION**

### **Principle 5: Protection of Opinion**

No one may be subjected to any sort of restraint, disadvantage or sanction because of his or her opinions or beliefs.

### **Principle 6: Expression That May Threaten National Security**

Subject to Principles 15 and 16, expression may be punished as a threat to national security only if a government can demonstrate that:

(a) the expression is intended to incite imminent violence; (b) it is likely to incite such violence; and (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.

### **Principle 7: Protected Expression**

- (a) Subject to Principles 15 and 16, the peaceful exercise of the right to freedom of expression shall not be considered a threat to national security or subjected to any restrictions or penalties. Expression which shall not constitute a threat to national security includes, but is not limited to, expression that:
- (i) advocates non-violent change of government policy or the government itself;
  - (ii) constitutes criticism of, or insult to, the nation, the state or its symbols, the government, its agencies, or public officials, or a foreign nation, state or its symbols, government, agencies or public officials;
  - (iii) constitutes objection, or advocacy of objection, on grounds of religion, conscience or belief, to military conscription or service, a particular conflict, or the threat or use of force to settle international disputes;
  - (iv) is directed at communicating information about alleged violations of international human rights standards or international humanitarian law.

- (b) No one may be punished for criticizing or insulting the nation, the state or its symbols, the government, its agencies, or public officials, or a foreign nation, state or its symbols, government, agency or public official unless the criticism or insult was intended and likely to incite imminent violence.

### **Principle 8: Mere Publicity of Activities That May Threaten National Security**

Expression may not be prevented or punished merely because it transmits information issued by or about an organization that a government has declared threatens national security or a related interest.

### **Principle 9: Use of a Minority or Other Language**

Expression, whether written or oral, can never be prohibited on the ground that it is in a particular language, especially the language of a national minority.

### **Principle 10: Unlawful Interference With Expression by Third Parties**

Governments are obliged to take reasonable measures to prevent private groups or individuals from interfering unlawfully with the peaceful exercise of freedom of expression, even where the expression is critical of the government or its policies. In particular, governments are obliged to condemn unlawful actions aimed at silencing freedom of expression, and to investigate and bring to justice those responsible.

## **III. RESTRICTIONS ON FREEDOM OF INFORMATION**

### **Principle 11: General Rule on Access to Information**

Everyone has the right to obtain information from public authorities, including information relating to national security. No restriction on this right may be imposed on the ground of national security unless the government can demonstrate that the restriction is prescribed by law and is necessary in a democratic society to protect a legitimate national security interest.

### **Principle 12: Narrow Designation of Security Exemption**

A state may not categorically deny access to all information related to national security, but must designate in law only those specific and narrow categories of information that it is necessary to withhold in order to protect a legitimate national security interest.

### **Principle 13: Public Interest in Disclosure**

In all laws and decisions concerning the right to obtain information, the public interest in knowing the information shall be a primary consideration.

### **Principle 14: Right to Independent Review of Denial of Information**

The state is obliged to adopt appropriate measures to give effect to the right to obtain information. These measures shall require the authorities, if they deny a request for information, to specify their reasons for doing so in writing and as soon as reasonably possible; and shall provide for a right of review of the merits and the validity of the denial by an independent authority, including some form of judicial review of the legality of the denial. The reviewing authority must have the right to examine the information withheld.

### **Principle 15: General Rule on Disclosure of Secret Information**

No person may be punished on national security grounds for disclosure of information if (1) the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or (2) the public interest in knowing the information outweighs the harm from disclosure.

### **Principle 16: Information Obtained Through Public Service**

No person may be subjected to any detriment on national security grounds for disclosing information that he or she learned by virtue of government service if the public interest in knowing the information outweighs the harm from disclosure.

### **Principle 17: Information in the Public Domain**

Once information has been made generally available, by whatever means, whether or not lawful, any justification for trying to stop further publication will be overridden by the public's right to know.

### **Principle 18: Protection of Journalists' Sources**

Protection of national security may not be used as a reason to compel a journalist to reveal a confidential source.

**Principle 19: Access to Restricted Areas**

Any restriction on the free flow of information may not be of such a nature as to thwart the purposes of human rights and humanitarian law. In particular, governments may not prevent journalists or representatives of intergovernmental or non-governmental organizations with a mandate to monitor adherence to human rights or humanitarian standards from entering areas where there are reasonable grounds to believe that violations of human rights or humanitarian law are being, or have been, committed. Governments may not exclude journalists or representatives of such organizations from areas that are experiencing violence or armed conflict except where their presence would pose a clear risk to the safety of others.

**IV. RULE OF LAW AND OTHER MATTERS**

**Principle 20: General Rule of Law Protections**

Any person accused of a security-related crime involving expression or information is entitled to all of the rule of law protections that are part of international law. These include, but are not limited to, the following rights:

(a) the right to be presumed innocent; (b) the right not to be arbitrarily detained; (c) the right to be informed promptly in a language the person can understand of the charges and the supporting evidence against him or her; (d) the right to prompt access to counsel of choice; (e) the right to a trial within a reasonable time; (f) the right to have adequate time to prepare his or her defence; (g) the right to a fair and public trial by an independent and impartial court or tribunal; (h) the right to examine prosecution witnesses; (i) the right not to have evidence introduced at trial unless it has been disclosed to the accused and he or she has had an opportunity to rebut it; and (j) the right to appeal to an independent court or tribunal with power to review the decision on law and facts and set it aside.

**Principle 21: Remedies**

All remedies, including special ones, such as habeas corpus or amparo, shall be available to persons charged with security-related crimes, including during public emergencies which threaten the life of the country, as defined in Principle 3.

**Principle 22: Right to Trial by an Independent Tribunal**

(a) At the option of the accused, a criminal prosecution of a security-related crime should be tried by a jury where that institution exists or else by judges who are genuinely independent. The trial of persons accused of security-related crimes by judges without security of tenure constitutes a *prima facie* violation of the right to be tried by an independent tribunal.

(b) In no case may a civilian be tried for a security-related crime by a military court or tribunal.

(c) In no case may a civilian or member of the military be tried by an ad hoc or specially constituted national court or tribunal.

**Principle 23: Prior Censorship**

Expression shall not be subject to prior censorship in the interest of protecting national security, except in time of public emergency which threatens the life of the country under the conditions stated in Principle 3.

**Principle 24: Disproportionate Punishments**

A person, media outlet, political or other organization may not be subject to such sanctions, restraints or penalties for a security-related crime involving freedom of expression or information that are disproportionate to the seriousness of the actual crime.

**Principle 25: Relation of These Principles to Other Standards**

Nothing in these Principles may be interpreted as restricting or limiting any human rights or freedoms recognized in international, regional or national law or standards.

# Principles on Freedom of Information Legislation (1999)<sup>15</sup>

Article 19, 1999

## PRINCIPLE 1. MAXIMUM DISCLOSURE

*Freedom of information legislation should be guided by the principle of maximum disclosure*

The principle of maximum disclosure establishes a presumption that all information held by public bodies should be subject to disclosure and that this presumption may be overcome only in very limited circumstances (see Principle 4). This principle encapsulates the basic rationale underlying the very concept of freedom of information and ideally it should be provided for in the Constitution to make it clear that access to official information is a basic right. The overriding goal of legislation should be to implement maximum disclosure in practice.

Public bodies have an obligation to disclose information and every member of the public has a corresponding right to receive information. Everyone present in the territory of the country should benefit from this right. The exercise of this right should not require individuals to demonstrate a specific interest in the information. Where a public authority seeks to deny access to information, it should bear the onus of justifying the refusal at each stage of the proceedings. In other words, the public authority must show that the information which it wishes to withhold comes within the scope of the limited regime of exceptions, as detailed below.

### Definitions

Both 'information' and 'public bodies' should be defined broadly.

<sup>15</sup> Source: Mendel, Toby, Parliament and Access to Information. Working for Transparent Governance, Washington: World Bank Institute, 2005.

'Information' includes all records held by a public body, regardless of the form in which the information is stored (document, tape, electronic recording and so on), its source (whether it was produced by the public body or some other body) and the date of production. The legislation should also apply to records which have been classified, subjecting them to the same test as all other records.

For purposes of disclosure of information, the definition of 'public body' should focus on the type of service provided rather than on formal designations. To this end, it should include all branches and levels of government including local government, elected bodies, bodies which operate under a statutory mandate, nationalised industries and public corporations, non-departmental bodies or quangos (quasi non-governmental organisations), judicial bodies, and private bodies which carry out public functions (such as maintaining roads or operating rail lines). Private bodies themselves should also be included if they hold information whose disclosure is likely to diminish the risk of harm to key public interests, such as the environment and health. Inter-governmental organizations should also be subject to freedom of information regimes based on the principles set down in this document.

### Destruction of records

To protect the integrity and availability of records, the law should provide that obstruction of access to, or the wilful destruction of records is a criminal offence. The law should also establish minimum standards regarding the maintenance and preservation of records by public bodies. Such bodies should be required to allocate sufficient resources and attention to ensuring that public record-keeping is

## **Access to Information and Security Sector Governance**

adequate. In addition, to prevent any attempt to doctor or otherwise alter records, the obligation to disclose should apply to records themselves and not just the information they contain.

### **PRINCIPLE 2. OBLIGATION TO PUBLISH**

*Public bodies should be under an obligation to publish key information*

Freedom of information implies not only that public bodies accede to requests for information but also that they publish and disseminate widely documents of significant public interest, subject only to reasonable limits based on resources and capacity. Which information should be published will depend on the public body concerned. The law should establish both a general obligation to publish and key categories of information that must be published.

Public bodies should, as a minimum, be under an obligation to publish the following categories of information:

- operational information about how the public body functions, including costs, objectives, audited accounts, standards, achievements and so on, particularly where the body provides direct services to the public;
- information on any requests, complaints or other direct actions which members of the public may take in relation to the public body;
- guidance on processes by which members of the public may provide input into major policy or legislative proposals;
- the types of information which the body holds and the form in which this information is held; and
- the content of any decision or policy affecting the public, along with reasons for the decision and background material of importance in framing the decision.

### **PRINCIPLE 3. PROMOTION OF OPEN GOVERNMENT**

*Public bodies must actively promote open government*

Informing the public of their rights and promoting a culture of openness within government are essential if the goals of freedom of information legislation are to be realised. Indeed, experience in various countries shows that a recalcitrant civil service can undermine even the most progressive legislation. Promotional activities are, therefore, an essential component of a freedom of information regime. This is an area where the particular activities will vary from country to country, depending on factors such as the way the civil service is organised, key constraints to the free disclosure of information, literacy levels and the degree of awareness of the general public. The law should require that adequate resources and attention are devoted to the question of promoting the goals of the legislation.

#### **Public Education**

As a minimum, the law should make provision for public education and the dissemination of information regarding the right to access information, the scope of information which is available and the manner in which such rights may be exercised. In countries where newspaper distribution or literacy levels are low, the broadcast media are a particularly important vehicle for such dissemination and education. Creative alternatives, such as town meetings or mobile film units, should be explored. Ideally, such activities should be undertaken both by individual public bodies and a specially designated and adequately funded official body – either the one which reviews requests for information, or another body established specifically for this purpose.

#### **Tackling the culture of official secrecy**

The law should provide for a number of mechanisms to address the problem of a culture of secrecy within government. These should include a requirement that public bodies provide freedom of information training for their employees. Such training should address the importance and scope of freedom of information, procedural mechanisms for

accessing information, how to maintain and access records efficiently, the scope of whistleblower protection, and what sort of information a body is required to publish.

The official body responsible for public education should also play a role in promoting openness within government. Initiatives might include incentives for public bodies that perform well, campaigns to address secrecy problems and communications campaigns encouraging bodies that are improving and criticising those which remain excessively secret. Another possibility is the production of an annual report to Parliament and/or Parliamentary bodies on remaining problems and achievements, which might also include measures taken to improve public access to information, any remaining constraints to the free flow of information which have been identified and measures to be taken in the year ahead. Public bodies should be encouraged to adopt internal codes on access and openness.

#### **PRINCIPLE 4. LIMITED SCOPE OF EXCEPTIONS**

*Exceptions should be clearly and narrowly drawn and subject to strict “harm” and “public interest” tests*

All individual requests for information from public bodies should be met unless the public body can show that the information falls within the scope of the limited regime of exceptions. A refusal to disclose information is not justified unless the public authority can show that the information meets a strict three-part test.

The three-part test:

- the information must relate to a legitimate aim listed in the law;
- disclosure must threaten to cause substantial harm to that aim; and
- the harm to the aim must be greater than the public interest in having the information.

No public bodies should be completely excluded from the ambit of the law, even if the majority of their functions fall within the zone of exceptions. This applies to all branches of government (that is, the executive, legislative

and judicial branches) as well as to all functions of government (including, for example, functions of security and defence bodies). Non-disclosure of information must be justified on a case-by-case basis.

Restrictions whose aim is to protect governments from embarrassment or the exposure of wrongdoing can never be justified.

#### **Legitimate aims justifying exceptions**

A complete list of the legitimate aims which may justify non-disclosure should be provided in the law. This list should include only interests which constitute legitimate grounds for refusing to disclose documents and should be limited to matters such as law enforcement, privacy, national security, commercial and other confidentiality, public or individual safety, and the effectiveness and integrity of government decision-making processes.

Exceptions should be narrowly drawn so as to avoid including material which does not harm the legitimate interest. They should be based on the content, rather than the type, of the document. To meet this standard exceptions should, where relevant, be time-limited. For example, the justification for classifying information on the basis of national security may well disappear after a specific national security threat subsides.

#### **Refusals must meet a substantial harm test**

It is not sufficient that information simply fall within the scope of a legitimate aim listed in the law. The public body must also show that the disclosure of the information would cause substantial harm to that legitimate aim. In some cases, disclosure may benefit as well as harm the aim. For example, the exposure of corruption in the military may at first sight appear to weaken national defence but actually, over time, help to eliminate the corruption and strengthen the armed forces. For non-disclosure to be legitimate in such cases, the net effect of disclosure must be to cause substantial harm to the aim.

#### **Overriding public interest**

Even if it can be shown that disclosure of the information would cause substantial harm

## **Access to Information and Security Sector Governance**

to a legitimate aim, the information should still be disclosed if the benefits of disclosure outweigh the harm. For example, certain information may be private in nature but at the same time expose high-level corruption within government. The harm to the legitimate aim must be weighed against the public interest in having the information made public. Where the latter is greater, the law should provide for disclosure of the information.

### **PRINCIPLE 5. PROCESSES TO FACILITATE ACCESS**

*Requests for information should be processed rapidly and fairly and an independent review of any refusals should be available*

A process for deciding upon requests for information should be specified at three different levels: within the public body; appeals to an independent administrative body; and appeals to the courts. Where necessary, provision should be made to ensure full access to information for certain groups, for example those who cannot read or write, those who do not speak the language of the record, or those who suffer from disabilities such as blindness.

All public bodies should be required to establish open, accessible internal systems for ensuring the public's right to receive information. Generally, bodies should designate an individual who is responsible for processing such requests and for ensuring compliance with the law.

Public bodies should also be required to assist applicants whose requests relate to published information, or are unclear, excessively broad or otherwise in need of reformulation. On the other hand, public bodies should be able to refuse frivolous or vexatious requests. Public bodies should not have to provide individuals with information that is contained in a publication, but in such cases the body should direct the applicant to the published source.

The law should provide for strict time limits for the processing of requests and require that any refusals be accompanied by substantive written reasons.

### **Appeals**

Wherever practical, provision should be made for an internal appeal to a designated higher authority within the public authority who can review the original decision.

In all cases, the law should provide for an individual right of appeal to an independent administrative body from a refusal by a public body to disclose information. This may be either an existing body, such as an Ombudsman or Human Rights Commission, or one specially established for this purpose. In either case, the body must meet certain standards and have certain powers. Its independence should be guaranteed, both formally and through the process by which the head and/or board is/are appointed.

Appointments should be made by representative bodies, such as an all-party parliamentary committee, and the process should be open and allow for public input, for example regarding nominations. Individuals appointed to such a body should be required to meet strict standards of professionalism, independence and competence, and be subject to strict conflict of interest rules.

The procedure by which the administrative body processes appeals over requests for information which have been refused should be designed to operate rapidly and cost as little as is reasonably possible. This ensures that all members of the public can access this procedure and that excessive delays do not undermine the whole purpose of requesting information in the first place.

The administrative body should be granted full powers to investigate any appeal, including the ability to compel witnesses and, importantly, to require the public body to provide it with any information or record for its consideration, *in camera* where necessary and justified.

Upon the conclusion of an investigation, the administrative body should have the power to dismiss the appeal, to require the public body to disclose the information, to adjust any charges levied by the public body, to fine public bodies for obstructive behavior where warranted and/or to impose costs on public bodies in relation to the appeal.

The administrative body should also have the power to refer to the courts cases which disclose evidence of criminal obstruction of access to or wilful destruction of records.

Both the applicant and the public body should be able to appeal to the courts against decisions of the administrative body. Such appeals should include full power to review the case on its merits and not be limited to the question of whether the administrative body has acted reasonably. This will ensure that due attention is given to resolving difficult questions and that a consistent approach to freedom of expression issues is promoted.

## **PRINCIPLE 6. COSTS**

*Individuals should not be deterred from making requests for information by excessive costs*

The cost of gaining access to information held by public bodies should not be so high as to deter potential applicants, given that the whole rationale behind freedom of information laws is to promote open access to information. It is well established that the long-term benefits of openness far exceed the costs. In any case, experience in a number of countries suggests that access costs are not an effective means of offsetting the costs of a freedom of information regime.

Differing systems have been employed around the world to ensure that costs do not act as a deterrent to requests for information. In some jurisdictions, a two-tier system has been used, involving flat fees for each request, along with graduated fees depending on the actual cost of retrieving and providing the information. The latter should be waived or significantly reduced for requests for personal information or for requests in the public interest (which should be presumed where the purpose of the request is connected with publication). In some jurisdictions, higher fees are levied on commercial requests as a means of subsidising public interest requests.

## **PRINCIPLE 7. OPEN MEETINGS**

*Meetings of public bodies should be open to the public*

Freedom of information includes the public's right to know what the government is doing on its behalf and to participate in decision-making processes. Freedom of information legislation should therefore establish a presumption that all meetings of governing bodies are open to the public.

"Governing" in this context refers primarily to the exercise of decision-making powers, so bodies which merely proffer advice would not be covered. Political committees – meetings of members of the same political party – are not considered to be governing bodies.

On the other hand, meetings of elected bodies and their committees, planning and zoning boards, boards of public and educational authorities and public industrial development agencies would be included.

A "meeting" in this context refers primarily to a formal meeting, namely the official convening of a public body for the purpose of conducting public business. Factors that indicate that a meeting is formal are the requirement for a quorum and the applicability of formal procedural rules.

Notice of meetings is necessary if the public is to have a real opportunity to participate and the law should require that adequate notice of meetings is given sufficiently in advance to allow for attendance.

Meetings may be closed, but only in accordance with established procedures and where adequate reasons for closure exist. Any decision to close a meeting should itself be open to the public. The grounds for closure are broader than the list of exceptions to the rule of disclosure but are not unlimited. Reasons for closure might, in appropriate circumstances, include public health and safety, law enforcement or investigation, employee or personnel matters, privacy, commercial matters and national security.

## **PRINCIPLE 8. DISCLOSURE TAKES PRECEDENCE**

*Laws which are inconsistent with the principle of maximum disclosure should be amended or repealed*

## **Access to Information and Security Sector Governance**

The law on freedom of information should require that other legislation be interpreted, as far as possible, in a manner consistent with its provisions. Where this is not possible, other legislation dealing with publicly-held information should be subject to the principles underlying the freedom of information legislation.

The regime of exceptions provided for in the freedom of information law should be comprehensive and other laws should not be permitted to extend it. In particular, secrecy laws should not make it illegal for officials to divulge information which they are required to disclose under the freedom of information law.

Over the longer term, a commitment should be made to bring all laws relating to information into line with the principles underpinning the freedom of information law.

In addition, officials should be protected from sanctions where they have, reasonably and in good faith, disclosed information pursuant to a freedom of information request, even if it subsequently transpires that the information is not subject to disclosure. Otherwise, the culture of secrecy which envelopes many governing bodies will be maintained as officials may be excessively cautious about requests for information, to avoid any personal risk.

protection should apply even where disclosure would otherwise be in breach of a legal or employment requirement.

In some countries, protection for whistleblowers is conditional upon a requirement to release the information to certain individuals or oversight bodies. While this is generally appropriate, protection should also be available, where the public interest demands, in the context of disclosure to other individuals or even to the media.

The “public interest” in this context would include situations where the benefits of disclosure outweigh the harm, or where an alternative means of releasing the information is necessary to protect a key interest. This would apply, for example, in situations where whistleblowers need protection from retaliation, where the problem is unlikely to be resolved through formal mechanisms, where there is an exceptionally serious reason for releasing the information, such as an imminent threat to public health or safety, or where there is a risk that evidence of wrongdoing will otherwise be concealed or destroyed.

### **PRINCIPLE 9. PROTECTION FOR WHISTLEBLOWERS**

*Individuals who release information on wrongdoing – whistleblowers – must be protected*

Individuals should be protected from any legal, administrative or employment-related sanctions for releasing information on wrongdoing.

“Wrongdoing” in this context includes the commission of a criminal offence, failure to comply with a legal obligation, a miscarriage of justice, corruption or dishonesty, or serious maladministration regarding a public body. It also includes a serious threat to health, safety or the environment, whether linked to individual wrongdoing or not. Whistleblowers should benefit from protection as long as they acted in good faith and in the reasonable belief that the information was substantially true and disclosed evidence of wrongdoing. Such



## **مركز جنيف للرقابة الديموقراطية على القوات المسلحة**

شارع المعارف ٣٤  
رام الله / البيرة  
الضفة الغربية  
فلسطين

تلفون: ٠٠٩٧٢ (٢) ٢٩٥ ٦٢٩٧  
فاكس: ٠٠ ٩٧٢ (٢) ٢٩٥ ٦٢٩٥

## **مكتب بيروت**

مركز جفينور - بلوك ج - الطابق السادس  
شارع كليمونسو  
بيروت  
لبنان

تلفون: +٩٦١ (٠) ١ ٧٣٨ ٤٠١  
فاكس: +٩٦١ (٠) ١ ٧٣٨ ٤٠٢

### **DCAF Head Office, Geneva**

#### **By Post:**

Geneva Centre for the Democratic Control of Armed Forces (DCAF)  
P.O.Box 1360  
CH-1211 Geneva 1  
Switzerland

#### **For Visitors:**

Geneva Centre for the Democratic Control of Armed Forces (DCAF)  
Rue de Chantepoulet 11  
CH-1201 Geneva 1  
Switzerland

Tel: +41 (0) 22 741 77 00  
Fax:+41 (0) 22 741 77 05

### **DCAF Ramallah**

Al-Maaref Street 34  
Ramallah / Al-Bireh  
West Bank  
Palestine

Tel: +972 (2) 295 6297  
Fax: +972 (2) 295 6295

### **DCAF Beirut**

Gefinor Center - Block C - 6th Floor  
Clemenceau Street  
Beirut  
Lebanon

Tel: +961 (0) 1 738 401  
Fax: +961 (0) 1 738 402