

GENERAL ASSEMBLY



FIFTIETH REGULAR SESSION
October 20 to 21, 2020
Washington, D.C., United States of America
VIRTUAL

OEA/Ser.P
AG/doc.5718/20
18 November 2020
Original: Spanish

INTER-AMERICAN MODEL LAW 2.0 ON ACCESS TO PUBLIC INFORMATION

Adopted at the fourth plenary session, held on October 21, 2020, by operative paragraph 4 of
Section xi “Access to public information and protection of personal data” of
resolution AG/RES. 2958 (L-O/20), “Strengthening Democracy”

Explanatory Note

This document constitutes the conclusion of the work carried out by the Department of International Law (DIL) of the Secretariat for Legal Affairs in compliance with OAS General Assembly resolution AG/RES. 2905 (XLVII-O/17), *Strengthening Democracy* paragraph (ix). The resolution directs the DIL to “consult with the focal points of the Inter-American Program on Access to Public Information^{1/} as well as civil society, to identify the thematic areas that require updates or further development in the Model Inter-American Law on Access to Public Information (“the Model Law”), adopted by the General Assembly in 2010,^{2/} and to convey the results of this process to the Inter-American Juridical Committee for consideration and further development”.

In order to best fulfill its mandate, the DIL executed the activities that have been reported^{3/} to the Inter-American Juridical Committee (CJI) in a timely and detailed manner, including:

- ❖ conducting a survey, sent out to more than 4,000 individuals and institutions, including the Inter-American Commission of Women (CIM), the Inter-American Commission on Human Rights (IACHR) aimed at identifying the areas where the Model Law could be further developed;
- ❖ organizing four workshops held between April 2018 and May 2019, which were attended by 152 specialists from CSOs as well as authorities from 15 Member States, including many focal points of the Inter-American Program on Access to Public Information, as well as civil society organizations (CSOs); and
- ❖ organizing meetings to collect input and specific recommendations from 26 CSOs from 14 Member States: Argentina, Brazil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Paraguay, the United States, Uruguay and Venezuela.

The most commonly identified areas as priorities for revision were: exceptions regime, active transparency, document management, guarantor bodies, political parties and public information within the judiciary branch, all of which became the focus and substance of the workshops held with the guarantor bodies and civil society. In that context, three action items were decided by consensus:

- ❖ focus the collective efforts in the development of agreed upon texts on guarantor bodies, exceptions regime, subject entities, active transparency, definition and scope of the right of access to public information;
- ❖ to leave the matter of document and management in the hands of expert consultants, as the highly technical content of a model law would require very specialized knowledge; and attach to the revised draft Inter-American Model Law on Access to Public Information (Model Law 2.0) a proposed Model Law on Document Management and its Application Guide, thought these two latter documents would not technically be a part of the Model Law 2.0; and
- ❖ to postpone the discussion of the issue of access to public information in the possession or custody of the judiciary for another time, incorporating the input of information officers from the judicial branches and experts that may contribute a more comprehensive perspective of the particular

1. AG/RES. 2885 (XLVI-O/16)

2. AG/RES. 2607 (XL-O/10)

3. Document DDI/Doc.3/19 Rev.1

intricacies of the judicial processes, among them the need for classifying certain information at specific moments in the process, the implications of disclosure on the protection of victims, witnesses and minors, etc.

It is important to highlight that throughout this undertaking, the DIL has remained mindful of the gender perspective, recognizing the opportunity to propose provisions that make the Model Law 2.0 one of the first legal instruments of the Inter-American System to incorporate a gender perspective by design. To this end, a dedicated workshop was held exclusively to analyze issues pertaining to gender and access to information, with the participation of specialists whose contributions greatly enriched the agreed upon texts.

In July 2019, the DIL submitted a document^{4/} for the consideration of the members of the CJI including all the agreed upon provisions and invited them to submit their comments in writing. As no such comments were received, the DIL proceeded to assemble this document, which consolidates the original text of the Model Law that will remain unchanged with the agreed upon provisions on the areas identified during the consultation process as ripe for updates or enhancements.

By submitting this complete draft Model Law 2.0 to the consideration of the CJI during its 96th regular session, the DIL thereby has fulfilled the mandate conferred by the General Assembly.

4. Document DDI/Doc.3/19 Rev.1

**INTER-AMERICAN MODEL LAW 2.0
ON ACCESS TO PUBLIC INFORMATION**

TABLE OF CONTENTS

CHAPTER I. DEFINITIONS, SCOPE, RIGHT OF ACCESS AND INTERPRETATION

Definitions
Scope and purpose
Right of access to public Information
Interpretation

CHAPTER II. MEASURES TO PROMOTE OPENNESS

Active transparency
Classes of key information subject to proactive disclosure
Responsibilities of the subject entity with regard to active transparency
Publication schemes
Other laws and mechanisms
Previously disclosed information

CHAPTER III. ACCESSING INFORMATION HELD BY PUBLIC AUTHORITIES

Request for Information
Requirements of requests for Information
Interpretation of requests for Information
Forwarding requests for Information
Third party response to notification
Cost of reproduction
Display of Documents
Information Officer
Document search
Document management
Missing Information
Response period
Extension
Notice to the requester

CHAPTER IV. EXCEPTIONS REGIME

Exceptions to Disclosure
Supremacy of the Public Interest
Human rights
Acts of corruption
Entity responsible for classification
Generic classifications

Authority to declassify
Confidential Information
Reserved Information
Defense and national security
Harm Test
Public Interest test
Generalities of classification
Classification of Information
Declaration of confidentiality
Declaration of reserve
Declassification of Information
Revision of the exceptions regime
Registry of classified Information
Partial disclosure
Maximum duration of reserve
Non-Existent Information
Filing of appeals
Recourse against a failure to respond
Other laws

CHAPTER V. APPEALS

Internal appeal
External appeal
Resolution
Judicial review
Burden of proof

CHAPTER VI. GUARANTOR BODY

Creation
Characteristics
Composition
Requirements to be a commissioner
Selection procedure
Obligations of commissioners
Term of office
Removal or suspension of commissioners
Duties and powers of Guarantor Body
Budget
Reports of subject entities
Reports of the Guarantor Body
Civil and criminal liability
Administrative offenses

CHAPTER VII. PROMOTIONAL AND COMPLIANCE MEASURES

Monitoring and compliance

Training

Formal Education

CHAPTER VIII. TRANSITORY PROVISIONS

Abbreviated title and entry into force

Regulations

INTER-AMERICAN MODEL LAW 2.0
ON ACCESS TO PUBLIC INFORMATION

CHAPTER I. DEFINITIONS, SCOPE, RIGHT OF ACCESS AND INTERPRETATION

Article 1. Definitions

In this Law, unless the context otherwise requires:

- a) “Public Interest Activity” refers to those subjects or areas of management that should be resolved in government political decisions, at any of the levels of administrative, legislative or judicial political organization, and that seek to serve the maximum interest of the community;
- b) “Senior Officials” refers to any official within a Public Authority whose total annual salary exceeds [USD\$100,000];
- c) “Public Authority” refers to any governmental authority and to the private organizations falling under the third paragraph of Article 2 of this Law;
- d) “Document” refers to any written Information, regardless of its form, source, date of creation or official status, whether or not it was created by a Public Authority, political parties, unions and non-profit organizations holding the document and whether or not it was classified as confidential;
- e) “Public Funds” refers to the financial resources, whether tax-related or not, that are generated, obtained, or originated by the State, regardless of who manages those resources;
- f) “Unions” refers to the association of persons and/or companies engaged in the same work and whose main objective is mutual support, wherein they seek the well-being of the group they represent;
- g) “Information” refers to any type of datum in the custody or control of a Public Authority, Political Party, Union and Non-Profit Organizations.
- h) “Personal Information” refers to information regarding a living person who is or may be identified through such Information;^{1/}
- i) “Information Officer” refers to the individual or individuals appointed by a Public Authority pursuant to Article 18 of this Law;
- j) “Non-profit organization” refers to entities recognized by the State that engage in activities designed to serve the public interest, whose purpose is not to make a profit, that have a specific mission and are independent of the State.
- k) “Political Party” refers to public interest entities with their own legal status and assets, recognized by national legislation, the purpose of which is to promote the people’s participation in democratic life, contribute to the formation of representative political bodies

1. This definition has been taken from the Principles on Privacy and Personal Data Protection in the Americas, approved during the 84th Regular Session of the Inter-American Juridical Committee (CJI/doc. 450/14).

and, as citizen organizations of citizens, to enable citizen access to the exercise of public power;

- l) “Publish” refers to the act of making Information accessible to the general public and includes printing, broadcasting and electronic forms of dissemination; and
- m) “Interested Third Parties” refers to persons who have a direct interest in preventing the disclosure of Information they provided voluntarily to a Public Authority, because such disclosure either affects their privacy or their commercial interests.

Article 2. Scope and purpose

1. This Law establishes the broadest possible application of the right of access to Information that may be in the possession, custody or control of any Public Authority, Political Party, Union and Non-Profit Organization, and that is based on the principles of *pro homine* and *in dubio pro actione* in accordance with which one ought to seek the interpretation most favorable to the exercise of that right.

2. This Law is also based on the principle of maximum disclosure, so that any Information held by subject entities shall be complete, timely and accessible, subject to a clear and narrow exceptions regime to be defined by law as well as legitimate and strictly necessary in a democratic society.

3. This law applies to:

- a) any Public Authority belonging to any branch of government (executive, legislative and judicial) and at all levels of the internal governmental structure (central or federal, regional, provincial or municipal);
- b) independent or autonomous bodies, organizations or entities owned or controlled by the government, acting by virtue of powers granted by the Constitution or by other laws; and
- c) Public Funds, as well as any individual or legal entity that receives or manages public resources or carries out acts of authority at the national or federal level.^{2/}

3.1 This Law shall likewise apply to private organizations, Political Parties or similar associations, Unions, guilds and Non-Profit Organizations, which must respond to requests for Information but only with respect to the Public Funds or benefits received or the public functions and services performed. In the event that said Public Funds or benefits exceed [XX% of their annual budget / the amount of \$XX], the above entities shall also comply with the obligations of active transparency provided in this Law.

4. No public authority shall be exempt from the requirements established in this law, including the legislative and judicial branch, supervisory institutions, intelligence services, armed forces, police, other security bodies, Chiefs of State and government, and the divisions thereof.

Subject entities shall document any action deriving from the exercise of their powers, responsibilities or functions.

2. Comment: the term “public benefits” should not be interpreted broadly, so as to include any financial benefit received from the government.

5. In the event of any inconsistency, this Law shall prevail over any other law.^{3/}

Article 3. Right of access to public information

1. Any person requesting Information from any Public Authority covered by this Law shall have the following rights, subject only to the provisions of Chapter IV of this Law:
 - a) to be informed whether or not the Public Authority holds Documents containing the Information requested or from which that Information may be derived;
 - b) if the Public Authority that received the request holds said Documents, to be promptly notified accordingly;
 - c) if said Documents are not delivered to the requester, to appeal the failure to deliver the Information;
 - d) to make anonymous requests for Information;
 - e) to request Information without having to justify the reasons why it is being sought;
 - f) to be free from any discrimination that may be based on the nature of the request; and
 - g) to obtain the Information free of charge or at a cost not exceeding the cost to reproduce the Documents.
2. The requester shall not be sanctioned, punished or prosecuted for exercising the right of access to Information.
3. The Information Officer shall make reasonable efforts to assist the requester with regard to the request, to respond to the request accurately and completely and, subject to applicable regulations, to provide timely access to the Documents in the format requested.
4. The Guarantor Body shall make reasonable efforts to assist the requester in connection with an appeal filed in response to a refusal to disclose Information.^{4/}

Article 4. Interpretation

1. Anyone tasked with the interpretation of this Law, or any other legislation or regulatory instrument that may affect the right to Information shall adopt the reasonable interpretation that ensures the most effective right to information.
2. When several institutions have jurisdiction over access to public Information and the protection of personal data, close coordination should be sought so that both rights are harmoniously protected.

3. Comment: While the Model Law does not contain a provision that includes within its scope information in the possession of private companies that is necessary for the exercise or protection of internationally recognized human rights, it is noted that some states, including South Africa, have adopted this approach.

4. Comment: to meet this requirement, it is considered a good practice to make a free legal advisory service available to requesters who need it during the administrative or legal proceeding on access to public Information.

CHAPTER II. MEASURES TO PROMOTE OPENNESS

Article 5. Active transparency

1. All subject entities shall proactively disseminate the key Information established by this Law, without the need for any request for such Information.
2. All subject entities shall allow the broadest access to such Information so as to permit interoperability in an open data format^{5/} as well as determine strategies for the identification, generation, organization, publication and dissemination of such Information so that it can be easily reused^{6/} by society.
3. The Guarantor Body is responsible for:
 - a) periodically ensuring that subject entities fully implement these obligations;
 - b) designing policies that facilitate the coordination of efforts and tasks carried out by subject entities in order to comply with their active transparency obligations;^{7/}
 - c) issuing the technical guidelines it deems appropriate for establishing information publication formats so as to facilitate the proper standardization thereof and ensuring that such information is accurate, reliable, timely, consistent, comprehensive, updated, accessible, comprehensible, and verifiable and satisfies the principle of non-discrimination.
 - d) establishing the criteria and protocols for removing key information, ensuring in any case that access to the record of that Information remains available through other mechanisms; and
 - e) establishing the administrative sanctions corresponding to the head of the administrative unit of the subject entity in the event of a failure to fulfil these obligations.

Article 6. Classes of key Information subject to proactive disclosure

1. The following are the key classes of Information subject to proactive disclosure^{8/} by a subject entity:

A. General Information on the subject entity, including:

- a) a detailed description of services provided directly to the public, including Information on their standards and service protocols, as well as procedures to be followed and formats to be used for obtaining said services;

-
5. Comment: *Open data* is understood to mean data that can be used, reused and redistributed. They should be in a free and unrestricted format so that derivative services can be created from them.
 6. Comment: The objective of reusing Information is to share it among the largest number of people, using all available media including, *inter alia*, the website, broadcast media, television and the print media.
 7. Comment: The Guarantor Body should verify that declassified Information becomes actively published Information.
 8. Comment: The publication of this Information must be organized by subject, in sequential or chronological order, without grouping, generalizing or modifying concepts, so that people can be informed correctly and without confusion.

- b) a description of their organic structure, the location of their departments and offices, and hours of service to the public;
- c) strategic programs and work plans, as applicable, as well as the outcomes, outputs and impacts obtained in the performance of their work;
- d) file classification chart and the document arrangement catalogue or similar instruments.
- e) simple but complete description of procedures to be followed for making requests for Information and filing appeals as well as complaints regarding actions or omissions of the subject entity;
- f) relevant Information on the content of their publication schemes;
- g) all laws, regulations, resolutions, policies, guidelines or manuals or other documents containing interpretations, practices or precedents regarding the subject entity's performance of its functions, that affect the general public;
- h) reports that pursuant to legal provisions are generated in the performance of their powers, responsibilities or functions, broken down as much as possible;
- i) description of their internal and external oversight, reporting and monitoring mechanisms, as well as their governance codes and the content of audit reports;
- j) index of classified Information, as well as Information on the area responsible for that information;
- k) index of Information classified as confidential; and
- l) index of Information that has been recently declassified.

B. Information on public officials^{9/}

- a) Information on the total number of officials, their names, the positions they hold and their place in the hierarchy, as well as their roles and duties, all broken down by gender and other categories relevant to the role of the subject entity, particularly with reference to higher level positions;
- b) a detailed description of the powers and duties of the highest ranking officials, as well as the procedures they follow in adopting decisions;
- c) salary scales corresponding to all categories of officials, including all components and sub-components of their salaries. This Information should be updated whenever there are position reclassifications, salary increases or changes in the method of payment;

9. Comment: The following section applies to any public official understood as someone who receives Public Funds for his services, regardless of how hired and includes advisors and consultants.

- d) salaries, including bonuses, risk premiums, compensation in cash and in kind, and all other income from any source,^{10/} including Information on the existing gender-based salary gap;
- e) representation expenses and per-diems received;
- f) sworn statements of interests and assets, or their equivalent;
- g) names of officials who benefit from licenses, permits and concessions in general;
- h) mechanisms for evaluation of Senior Officials;
- i) calendars^{11/} of public officials who are in contact with the public;
- j) invitations to compete for public positions and consulting assignments, as well as the result of those processes;
- k) description of personnel selection and contracting procedures, regardless of the contract form.
- l) list of individuals or legal entities that for whatever reason are allowed to use public resources or carry out acts of authority, the amounts they utilize, the calls and criteria for their selection, as well as the reports that said persons submit on how those resources are used and allocated; and
- m) list of public officials who have been subject to firm and/or final administrative sanctions, specifying the reason for the sanction and the provisions on which the sanction was based.

C. Financial Information

- a) budget and spending plans corresponding to the current fiscal year as well as budgetary execution, breaking the information down by item, and indicating which specific projects and subsidies are intended to meet the needs of certain groups of society, including women;
- b) year-end account statements corresponding to prior years;
- c) description of procurement policies, guidelines and procedures, as well as contracts awarded;^{12/}
- d) Information on public works projects and projects that use Public Funds, generated during the planning, award, contracting, execution, supervision and liquidation stages, as well as the evaluation of results;
- e) Information on the beneficiaries of tax exemptions or tax incentives;

10. Comment: a record must be kept of donations that public servants may receive.

11. Comment: Information related to private meetings in which public servants participate must be disclosed, whether their purpose is lobbying, the management of particular interests with respect to the decisions they make or any other purpose.

12. Comment: To comply with this requirement, subject entities may make use of the OECD Council's "Recommendation on Fighting Bid Rigging in Public Procurement."

- f) studies, analyses, statistics and other similar documents produced with financing from public resources;
- g) financial management rules and control mechanisms;
- h) audit and other reports, prepared by agencies responsible for the supervision of financial aspects, including the principal performance indicators on how the budget is executed as well as a summary of classified sections as applicable;
- i) amounts assigned to expenses for any type of social communication and official publicity programs or campaigns, broken down by type of media, contract number and purpose;
- j) a list of companies and persons that have breached contracts with the subject entity; and
- k) Information on all outlays by the subject entity to publicize, promote, explain or defend a policy or decision.

D. Citizen Participation Mechanisms

- a) description of mechanisms or general procedures for citizen participation; the forms of citizen participation that are binding and open government in nature; and mechanisms for social control, social comptrollership, social oversight or the like directed to promoting citizen participation in accountability and in combating corruption, with respect to both subject entities and guarantor bodies;
- b) description of the results of the use and implementation of those mechanisms or procedures broken down by gender and age;
- c) repository of all requests made by persons as well as the responses made to them, for which subject entities shall create, publish and maintain on their website as well as in the reception area of all their offices accessible to the public, a log of requests and disclosures of all documents disseminated in response to requests made in accordance with this Law; and
- d) summary of all appeals, complaints or other actions filed by persons.

E. Needs of Specific Groups

- a) relevant Information needed to promote greater gender equity^{13/} such as calculation of the salary gap, information on existing programs benefiting women, statistics or indicators related to labor inclusion, health, and other aspects.
- b) relevant and necessary Information on social programs intended to meet the needs of other specific groups of society such as minors, seniors, afro-descendants, the lesbian, gay, bisexual,

13. Comment: The Transparency and Access to Information Network prepared a report called "Diagnostic and Methodological Study for Incorporating the Gender Perspective in Transparency and Access to Information Policies in Latin America," which could be an important input for meeting this requirement.

transgender and intersex (LGBTI) community and the members of indigenous community, as well as persons with disabilities.

- c) detailed Information on indicators of progress and statistics that can be used to verify compliance in the implementation of gender equity, as well as on meeting the needs of other specific groups of society, including the impact generated for such groups.
- d) list of subsidies granted to those sectors of society, broken down by group.
- e) other indicators related to issues of social impact that, consistent with their functions, they should disseminate.
- f) Information on the standards of human rights protection contained in international treaties, as well as recommendations, reports or resolutions issued by public agencies of the State or international organizations on the subject of human rights and the actions they have carried out for their implementation.

Article 7. Responsibilities of the subject entity with regard to active transparency

1. The subject entity should be sure to make available to those without Internet access a physical space with computer equipment and the assistance of qualified staff facilitating access to information in the entity's possession, custody or control.
2. Each subject entity shall appoint an Information Officer, who shall be responsible for complying with the active transparency requirement while adhering to the principles of gratuity, non-discrimination, timeliness, accessibility and integrity.^{14/}
3. The Information Officer should ensure that the information disclosed on websites can be processed and is in selectable format,^{15/} meaning that data can be copied electronically for later use or processing.
4. The Information Officer shall ensure that all Information published is accompanied by the date of its latest update.

14. Comment: The gratuity principle is understood to mean the principle whereby obtaining and consulting Information should be free of cost, with requesters paying only the value, when applicable, of the materials used or shipping costs.

The principle of non-discrimination is understood to mean that there should be no barriers to access to Information for all or any one of the reasons established in the Inter-American Convention against All Forms of Discrimination and Intolerance, adopted by the OAS in 2013.

The principle of timeliness is understood to mean that Information should be provided in the least amount of time possible, avoiding undue delays, through simple and expeditious procedures.

The principles of accessibility and integrity are understood to mean that the Information should be complete, comprehensible, useful, reliable, truthful and available in formats accessible through a simple and effective search system.

15. Comment: *Selectable format* means a free format that allows the Information to be reused.

5. The Information Officer shall ensure updating, at least every (three months), unless another provision establishes a different period, of the key Information published by the subject entity, taking into consideration the production cycles of such Information.

6. The Information Officer shall ensure the annual creation and filing of a digital image of the website that contains all the key Information and information established in the publication scheme.

Article 8. Publication schemes

1. In addition to the key information established in Article 6, any subject entity may design, adopt and implement a publication scheme containing Information in its possession, control or custody to be disseminated proactively without any specific request.

2. When designing and implementing its publication scheme, the subject entity shall take into consideration the need to:

- a) meet the citizens' most relevant needs for useful knowledge regarding that Information;
- b) minimize the need for individuals to submit requests regarding the Information;
- c) promote the gradual inclusion of Information, the periodic updating of these schemes, and their non-regression through the use of indicators of progress; and
- d) promote equality of opportunities for all sectors of the population, through the inclusion in publication schemes of Information that is useful and relevant to their particular interests and needs, such as that relevant to minors, women, the elderly, afro-descendants, the LGBTI community, and members of indigenous communities, as well as persons with disabilities, ensuring that the latter are provided reasonable adjustments with regard to accessibility mechanisms.

3. Subject entities shall inform the Guarantor Body of their publication schemes and that body may, if it deems advisable, make appropriate recommendations that shall be binding in nature. The publication schemes shall be updated on a gradual and ongoing basis.

4. The Guarantor Body shall have the authority and competence to determine whether or not the Information contained in the publication schemes is subject to the exceptions regime.

5. The Guarantor Body may approve model publication schemes for specific subject entities in order to harmonize such schemes, without prejudice to considering the particular characteristics and needs thereof.

Article 9. Other laws and mechanisms

1. This Law does not affect the operation of any other legislation that:

- a) requires that the Information contained in Documents in the possession, custody or control of the subject entity be available to the public;
- b) allows anyone to access to the Documents in the possession, custody or control of the subject entity;
- c) requires the publication of Information concerning the operations of the subject entity.

2. Whenever anyone makes a request for Information pursuant to that law or administrative act, said request shall be processed in an equally favorable manner as if it had been made under this Law.

Article 10. Previously disclosed Information

1. Subject entities shall, in the simplest way possible, guarantee and facilitate requesters' access to all previously disclosed records.
2. Requests for Information contained in logs of requests and disclosures shall be published without delay when that Information is in electronic format. If not, it shall be published no later than [three] business days following the submission of a request.
3. When the response to a request has been delivered in electronic format, it shall be made public immediately on the subject entity's website.
4. In the event the same Information is requested a second time, it shall be made public proactively on the subject entity's website, regardless of the format in which it is found.

CHAPTER III. ACCESSING INFORMATION HELD BY PUBLIC AUTHORITIES

Article 11. Request for Information

1. The request for Information may be filed in writing, by electronic means, verbally in person, by phone, or by any alternative means, with the relevant Information Officer. In all cases, the request shall be properly logged pursuant to Article 11.2 of this Law.
2. Unless the Information can be provided immediately, all requests shall be registered and assigned a tracking number, which shall be provided to the requester along with contact information for the Information Officer assigned to the request.
3. No fee shall be charged for making a request.
4. Requests for Information shall be registered in the order in which they are received and handled in a fair and non-discriminatory manner.

Article 12. Requirements of requests for Information

1. A request for Information shall contain the following:
 - a) contact information for the receipt of notices and delivery of the Information requested;
 - b) a sufficiently precise description of the requested Information, in order to allow for it to be located; and
 - c) the preferred form in which the Information is to be provided.

2. In the event that the form in which the Information is to be provided is not specified, the requested Information shall be delivered in the most efficient and cost-effective manner for the Public Authority^{16/}.

Article 13. Interpretation of requests for Information

1. The Public Authority in receipt of a request must reasonably interpret its scope and nature.

2. In the event that the receiving authority is uncertain as to the scope and nature of the requested Information, it must contact the requester for clarification. The receiving authority must make reasonable efforts to assist the requester in connection to the request, and respond accurately and completely.

Article 14. Forwarding requests for Information

1. If the receiving Public Authority reasonably determines that it is not the proper authority to handle the request, it must, as soon as possible and in any case within [five] working days, forward the request to the appropriate Public Authority for processing and notify the requester that his/her request has been routed to another Public Authority for processing.

3. The forwarding Public Authority must provide the requester with contact information for the Information Officer at the Public Authority where the request has been routed, in order to allow the requester to follow-up as needed.^{17/}

Article 15. Third party response to notification

Interested third parties shall be informed of the existence of a request for Information within [5] from the receipt thereof, and be given [10] days to make written representations to the receiving Public Authority either:

- a) consenting to disclosure of the requested Information; or
- b) stating the reasons why the Information should not be disclosed.

Article 16. Cost of reproduction

1. The requester shall only pay for the cost of reproduction of the requested Information and, if applicable, the cost of shipping, if so requested. Electronic delivery of Information shall be free of charge.

16. Comment: The requester need not provide their name on the request for Information. However, insofar as the request concerns personal Information, the requester's name may be required.

17. ALTERNATIVE: If the receiving Public Authority reasonably determines that it is not the proper authority to handle the request, it must, within the [five] business days following receipt of the request, identify the appropriate authority to the requester.

2. The cost of reproduction shall not exceed the actual cost of the material in which the Information is reproduced; cost of shipping shall not exceed the market value of same. For this purpose, the Guarantor Body shall periodically establish what they deem to be the fair market value.
3. The Public Authorities shall provide information free of all charges, including reproduction and shipping, for any low-income person as defined by the Guarantor Body.
4. The Guarantor Body will set additional rules regarding fees, which may include the possibility that the Information be provided free of charge if it is deemed to be in the public interest, or the possibility of setting a minimum number of pages to be delivered free of charge.

Article 17. Display of Documents

Public Authorities shall facilitate access to Documents by making the originals available for consultation in facilities suited for such purpose.

Article 18. Information Officer

1. The head of the Public Authority responsible for responding to requests must designate an Information Officer who shall be the focal point for implementing this law within said Public Authority. The contact information for each such Information Officer must be posted on the website of the Public Authority and made readily available to the public.
2. The Information Officer shall, in addition to any obligations specifically provided for in other sections of this Law, have the following:
 - a) to promote within the Public Authority the best possible practices in relation to the maintenance, archiving and disposal of Documents; and
 - b) to serve as a central contact within the Public Authority for receiving requests for Information, for assisting individuals seeking to obtain Information and for receiving individual complaints regarding the performance of the Public Authority in the disclosure of Information.

Article 19. Document search

Upon receipt of a request for Information, the Public Authority in receipt of the request must undertake a reasonable search for the Documents which best respond to the request.

Article 20. Document management

The [body responsible for archives] must develop, in coordination with the Guarantor Body, a Document management system which will be binding on all Public Authorities.

Article 21. Missing Information

When a Public Authority is unable to locate the Information responsive to a request, and records containing such Information should have been maintained, it shall be required to make reasonable efforts to gather the missing Information and deliver it to the requester.

Article 22. Response period

1. Each Public Authority must respond to a request for Information as soon as possible and in any event, within [twenty] working days of its receipt.
2. In the event that the request has been forwarded from one Public Authority to another, the effective date of receipt shall be that on which the appropriate authority received the forwarded request. In no event shall such date be greater than [ten] working days from the date in which the initial the request was first received by a Public Authority authorized to receive requests.

Article 23. Extension

1. Where a request for Information makes it necessary to search for or review a great deal of Documents, or the need to search offices physically separated from the receiving office, or the need to consult with other Public Authorities prior to reaching a determination on the disclosure of the requested Information, the Public Authority processing the request may extend the response time by up to an additional [twenty] business days.
2. In the event that the Public Authority fails to satisfy the request within [twenty] business days, or, if the conditions specified in paragraph 1 are met, the failure to respond to the request within [forty] business days shall be deemed a denial of the request.
3. In exceptional cases, involving large amounts of Information, the Public Authority may approach the Guarantor Body to request an extension greater than [forty] business days in order to respond to the request.
4. Where a Public Authority fails to meet the deadlines set forth in this article, no charge should be imposed for providing the Information. Furthermore, any Public Authority that fails to meet such deadlines must obtain prior authorization from the Guarantor Body to deny the Information or make a partial disclosure.
5. Under no circumstance may a third party notification excuse the Public Authority from complying with the terms and deadlines established in this law.

Article 24. Notice to the requester

1. As soon as the Public Authority has reasonable grounds to believe that satisfaction of a request will either incur reproduction charges in excess of the standards set by the Guarantor Body or take longer than [twenty] business days, it shall inform the requester and allow requester the opportunity to narrow or modify the scope of the request.
2. Public Authorities shall guarantee access to the Information in the form requested, unless this would:
 - a) harm the Document;
 - b) infringe on copyrights not held by Public Authority; or
 - c) be impractical because of the need to delete or redact some Information contained in the Document, pursuant to Chapter IV of this Law.

3. Where Information requested in electronic format is already available on the internet, the Public Authority may simply indicate the exact URL where the requester may access the Information.
4. Where the Information is requested in a non-electronic format, the Public Authority may not answer the request by making reference to a URL.
5. Where Information is provided to the requester, the latter shall be notified and informed of any applicable fees and/or arrangements for access.
6. In the event that all or part of the Information is withheld from a requester because it falls under the exceptions to disclosure under Chapter IV of this Law, the requester must be given:
 - a) a reasonable estimate of the volume of material that is being withheld;
 - b) a description of the precise provisions of this Law applied for the withholding; and
 - c) notification of the right to appeal.

CHAPTER IV. EXCEPTIONS REGIME

Article 25. Exceptions to disclosure

Subject entities may deny access to Public Information only under the assumptions considered in this chapter and under the following categories^{18/} of Information:

- a) Reserved Information: that public Information that is temporarily excluded from public knowledge due to a clear, probable and specific risk of damage to public interests and in compliance with the requirements specified in this Law.
- b) Confidential Information: that private Information held by subject entities to which public access is prohibited by constitutional or legal mandate due to a legally protected personal interest.

Article 26. Supremacy of the public interest

No subject entity may refuse to indicate whether or not a Document is in its power or refuse to disclose such Document, in accordance with the exceptions contained in Articles 32 and 33 hereunder, unless

18. Comment: The list of exceptions should be exhaustive and not include any clause extending these categories to “all others that may be established by legislation.”

the harm caused to the protected interest is greater than the public interest^{19/} of obtaining access to the Information.^{20/}

Article 27. Human rights

1. The exceptions contained in Article 33 may not be applied in cases of serious violations of human rights^{21/} or crimes against humanity.
2. In these cases the authority competent to qualify these acts as violating human rights shall be [the Guarantor Body], at the request of the subject entities or any person.
3. The competent authority shall protect the right to privacy of victims and shall employ the methods it deems necessary for this purpose, such as redacting or other similar mechanism.
4. Information related to violations of human rights is subject to a high presumption of disclosure; in no case may it be classified by invoking reasons of national security.^{22/}
5. In States subject to transitional justice processes, wherein truth, justice, reparation and there are guarantees of non-repetition, the integrity of all Documents that contain such Information must be protected and preserved and the documents must be published immediately.^{23/}

Article 28. Acts of corruption

1. The exceptions contained in Articles 32 and 33 may not be invoked in the case of Information related to acts of corruption by public officials as defined by current laws and the Inter-American Convention against Corruption.
2. In these cases the authority competent to qualify the Information as related to acts of corruption shall be [the Guarantor Body] at the request of the subject entities or any person.

19. Comment: *Information of public interest* refers to Information that proves to be relevant or beneficial to society and not simply of individual interest, the disclosure of which is useful so that the public understands the activities carried out by the subject entities, such as information referring to public health, the environment, public safety, socioeconomic and political matters and transparency in public management. This definition takes up the points included in the decision of the European Court of Human Rights in the SIOUTIS v. GREECE case.

20. Comment: Based on the principle of non-regression of public Information, a specific datum or Information of public interest that has already been disclosed in a specific format cannot cease to be made public based on a political decision.

21. Comment: This connotation may be expanded to encompass cases wherein the violation has not yet been established but there is a well-founded presumption or imminent threat that it will occur.

22. Comment: This article seeks to promote accountability for these violations, so that an effort is made to provide the victim with opportunities to gain access to effective reparations.

23. Comment: There is a preponderant public interest with regard to disclosing Information to society as a whole on the human rights violations committed under the previous regime.

Article 29. Entity responsible for classification

1. The [supreme authority of subject entity] shall be responsible for classifying Information, except as provided in Articles 32 and 33.^{24/}
2. Only specifically authorized or designated officials may classify Information. When an official without this power feels that certain Information should be classified, that Information may be considered classified for a brief period of no more than [5] business days until the designated official has reviewed the recommendation on classification.
3. The identity of the person responsible for a decision on classification must be reachable or identified in the Document, so as to ensure adequate accountability.
4. Public officials designated by law may delegate their original classification power to as few hierarchical subordinates as is viable from an administrative point of view.^{25/}

Article 30. Generic classifications

1. The classification of Information shall be an individual and case-based operation and subject entities shall not make generic classifications by law, decree, agreement or any other analogous instrument.
2. In no case may Information be classified before it has been generated.

Article 31. Authority to declassify

The Guarantor Body is empowered to order the declassification of information that does not meet the requirements set forth herein.

Article 32. Confidential Information

1. Subject entities may deny access to public Information when such access could harm the following private interests:
 - a) the right to privacy, including privacy related to life, health or safety, as well as the right to honor and to one's image;

24. Comment: A good practice is the creation of Transparency Committees, which may include the Information Officer, the heads of the Document management unit and the internal control body. Those committees meet periodically and their powers include the classification of information.

25. Comment: It is considered good practice to publish the number of persons authorized to classify Information, and the number of persons who have access to classified Information.

- b) personal data^{26/} that require the consent of their owner for their disclosure;
- c) legitimate commercial and economic interests;^{27/} and
- d) patents, copyrights and commercial secrets.

The public servants'^{28/} sphere of privacy is reduced according to their degree of responsibility. Consequently, public servants responsible for decision-making shall have a smaller sphere of privacy. Thus, in the event of conflict, the public interest shall prevail.

2. The exceptions in the preceding paragraph shall not apply when:

- a) the individual has expressly consented to the disclosure of his personal data;
- b) the circumstances of the case clearly indicate that the Information was delivered to the subject entity as part of the Information that should be subject to the disclosure regime;
- c) the Information is found in public records or publicly accessed sources;
- d) the Information is public in nature in accordance with this Law;
- e) there is a judicial order [that seeks] and/or [authorizes its publication];
- f) its publication is required for reasons of national security and general safety;
- g) when the Guarantor Body has ordered the declassification and disclosure of said Information;
- h) when it is transmitted among subject entities and between them and the subjects of international law, in terms of treaties and inter-institutional agreements, provided the Information is used for the exercise of those entities' own powers.

3. These exceptions shall not be applicable with respect to matters related to the functions of public officials, or when more than [20] years have passed since the death of the individual in question.

4. The heads of subject entities shall have knowledge of and maintain a registry of the public servants who based on the nature of their powers have access to the files and Documents classified as confidential. In addition, they shall ensure that said public servants are knowledgeable about their responsibility in the handling of classified Information.

5. Confidential Information shall remain confidential indefinitely, unless is it declassified by the Guarantor Body, in the case of personal data and with the consent of their owner, or when expressly determined by law.

26. Comment: Subject entities shall disclose Information in accordance with the provisions of the *Statement of Principles for Privacy and Personal Data Protection in the Americas* adopted by the Inter-American Juridical Committee at its eightieth regular session, through resolution CJI/RES. 186 (LXXX/O-12).

27. Comment: In cases where the Information on legitimate commercial and economic interests has been provided to the subject entity on a confidential basis, said Information shall remain exempt from disclosure.

28. Comment: The personal data of public servants are public to the extent that such data relate to the exercise of the position or inherent to the public service provided.

6. Once Information has been classified, the Guarantor Body is authorized and competent to verify whether the Information meets the requirements of classification; to fulfil this duty, it may view the Information. This power cannot be delegated.

Article 33. Reserved Information

1. Subject entities may deny access to public Information when there is a clear, probable and specific risk of significant harm. Reserved Information shall be that which:

- a) disrupts the future free and frank provision of advice within and among the subject entities;
- b) may undermine the conduct of international negotiations and relations;
- c) imperils anyone's life, human dignity, safety or health;
- d) contains opinions or recommendations that form part of the deliberative process of public servants, as long as a final decision has not been adopted;
- e) affects due process rights or undermines the conduct of judicial cases or administrative procedures, as long as they have not been decided;
- f) compromises the State's ability to manage the economy in the event of economic emergency decreed by law; and
- g) might cause serious harm to the activities of verification, inspection, audit,^{29/} investigation,^{30/} prevention or prosecution of crimes.

2. The exceptions contained in paragraphs a) and g) shall not apply to facts, the analysis of facts, technical information and statistics.

3. The exception under paragraph g) shall not be applied to the results of a particular examination or audit, once they have been completed.

4. Subject entities may deny access to public Information when allowing access would constitute a violation of restricted official communications, including legal Information that should be considered privileged.

5. If a document contains parts that should be rated as classified, the subject entity shall prepare public versions, deleting what is not suitable for disclosure.

Article 34. Defense and national security

1. The judicial branch, the legislative branch, chiefs of State and government, supervisory institutions, intelligence services, armed forces, police, and other security bodies may restrict the public's right to access Information when there are reasons of national security, but only when such

29. Comment: Once they are completed, audits constitute key Information and their dissemination must be proactive, i.e., without need for any requests for Information.

30. Comment: Information from completed investigations in cases that are not prosecuted shall be publicly accessible.

restrictions comply with all the other provisions established in this Law, and the requested Information falls under one of the following categories:

- a) Information on ongoing defense plans,^{31/} operations and issues of capacity during the period in which the Information has operational utility.^{32/}
- b) Information on the production, capacities or use of weapons systems^{33/} and other military systems, including communications systems.^{34/}
- c) Information on specific measures intended to safeguard the State's territory, critical infrastructure^{35/} or fundamental national institutions (*institutions essentielles*) against threats, use of force or sabotage, the effectiveness of which depends on restricting its disclosure.
- d) Information intrinsic to or derived from intelligence services' operations, sources and methods, provided they concern matters related to national security.
- e) Information related to matters of national security provided by a foreign State or intergovernmental agency with an express expectation of confidentiality and other diplomatic communications to the extent that they involve matters related to national security.

2. It is considered good practice for national legislation to establish an exclusive list of limited categories of information, such as the above.

Article 35. Harm test

1. When in response to a request for Information, delivery thereof is denied on the grounds that the Information is reserved, the subject entity shall apply the harm test.

2. The harm test must establish that the disclosure of Information may generate real, demonstrable and identifiable harm.^{36/}

31. Comment: Military operations that have already been carried out must be disclosed to third parties to ensure the right to the truth. In the event this Information has been destroyed, it shall be reconstructed by the competent authority.

32. Comment: It should be understood that the phrase "during the period in which the Information is of operational utility" requires disclosing the Information once it is assumed that this does not mean revealing data that could be utilized by enemies to learn the State's ability to react, its capacities, its plans, etc.

33. Comment: The States' maintenance and publication of a weapons control list is good practice encouraged by the Inter-American Convention on Transparency in Conventional Weapons Acquisition and the Arms Trade Treaty.

34. Comment: Said Information includes data and technological innovations and Information on production, capacity and use. Information on budget items related to weapons and other military systems should be available to the public.

35. Comment: "Critical infrastructure" refers to strategic resources, assets and systems, of such importance to the State that their destruction or incapacity would have a debilitating impact on national security.

36. Comment: The criteria of real, demonstrable and identifiable harm should be understood as follows:

In applying the harm test, the subject entity shall certify in writing that:

- a) the disclosure of Information represents a real, demonstrable and identifiable risk of significant injury to a legally protected right clearly identified in a law. A hypothetical harm or injury may not be used as justification;^{37/}
- b) the lack of a less harmful alternative to disclosure of the Information, to satisfy the public interest of disseminating the information;
- c) the risk of harm that such disclosure would involve exceeds the public interest in the dissemination of the Information;
- d) the limitation is consistent with the principle of proportionality^{38/} and represents the least restrictive means available for avoiding harm;
- e) the restriction does not subvert the very essence of the right to Information; and
- f) the concurrence of the requirements of timeliness, legality and reasonability.^{39/}

Real harm: The Information requested represents a real risk to the public interest; hypothetical harm cannot be used as a justification for secrecy.

Demonstrable harm: If said information were disclosed, it would entail greater damage to the public interest than if it were not provided.

Identifiable harm: The delivery of the Information would entail a greater impact on the parties involved in the events described above. Similarly, a public servant who improperly breaks the secrecy of proceedings or provides copy thereof or the Documents appearing in the investigation may be subject to an administrative or criminal liability procedure, as applicable.

37. Comment: It is not enough for the subject entity to argue that there is a risk of harm; it must also provide specific and substantial reasons supporting its assertions. The issuance of certificates or another similar type of instrument by a minister or other official does not constitute sufficient arguments to demonstrate that a legal good is affected.

38. Comment: Proportionality must be understood as the balance between harm and benefit to the public interest, so that the decision made represents a greater benefit than the harm it could cause to the population.

39. Comment: The requirements of timeliness, legality and reasonability must be understood in the following context:

- *Timeliness*: the reserve should be established for a specific period of time so that the reserved Information does not lose its public nature and thus when the grounds for the reserve disappear, the Information must be disseminated without restriction;
- *Legality*: the subject entity must conduct an analysis of the existing legal framework and demonstrate that the limits on the exercise of the right of access to public Information are aimed at protecting rights of similar or greater importance. In other words, it must prove that the requested Information falls under one of the grounds for exception provided in this Law; and
- *Reasonability*: it is not enough for the subject entity to cite legislation that authorizes it to deny the information because it considers it reserved. It must also justify the adoption of a limitation and provide a basis for the classification. This will reduce arbitrary action by public servants who have the power to classify information and will avoid unjustified denials of access to the Information.

4. The subject entity shall in all cases indicate the specific legal provision on which it bases the reserve.^{40/}

Article 36. Public Interest Test

1. When invoking the existence of grounds for confidentiality in response to a request for Information, the subject entity shall apply the public interest test.
2. The public interest test should be performed based on the elements of suitability, necessity and proportionality, when there is a collision of rights.

For these purposes, the following definitions shall apply:

- a) suitability: the legitimacy of the right adopted as prevailing. This must be appropriate to achieve a constitutionally valid purpose or suitable for achieving the intended purpose;
- b) necessity: the lack of less harmful alternatives for opening up the Information to satisfy a public interest.
- c) proportionality: the balance between the harm and benefit to the protected public interest, such that the decision represents a greater benefit to the population than the harm potentially caused by the disclosure and dissemination of the Information.

Article 37. Generalities of classification

Classification may be established partially or completely according to the content of the Information, and shall be consistent with the principles and provisions set forth in this Law.^{41/}

Article 38. Classification of Information

1. Prior to their adoption, the rules and procedures governing the classification of Information should be subject to a process of open consultation wherein people have the opportunity to express their proposals and observations.
2. The rules and procedures approved to govern classification must be broadly disseminated.
3. When the information has parts or sections that are reserved or confidential, in order to handle a request for Information, subject entities shall develop a public version in which classified parts or

40. Comment: In view of the burden of proof that Public Authorities have when reserved information, it is advisable to adopt rules (laws, regulations, guidelines, guides, agreements, etc.) that facilitate and specify the manner in which the harm test will be conducted, in that, on the one hand, Public Authorities would have a detailed procedure for its application and, on the other hand, individuals would have certainty regarding the elements that must be present in the reserve.

41. Comment: Subject entities may only classify Information that exists; classification may not predate the existence of the Information.

sections are redacted, providing a generic indication of their content and supporting and justifying their classification.

Article 39. Declaration of confidentiality

1. Confidential Information shall be classified in accordance with the public interest test.
2. The confidential nature of the Information held by subject entities shall be declared through an administrative action that should contain the following Information at a minimum:
 - a) date of the administrative classification action: corresponds to the date when the declaration of confidentiality was issued;
 - b) administrative office: the office that according to the of the subject entity's organizational chart generated or holds the confidential Information.
 - c) Information to be classified: individualized Information classified as confidential; indicating the case number, document, file, official letter, level, report, etc.
 - d) persons or agencies authorized to access that Information, preserving the confidential nature thereof, if any.
 - e) legal foundation: provisions of Article 32 supporting the classification.
 - f) justification: subject entities shall provide the motive for the classification being made, i.e., they shall specify the special reasons or circumstances that led them to conclude that the particular case falls within the assumptions provided in the Law.
 - g) signature of the public servant who authorizes the classification: act of the senior authority of the subject entity, of the person acting by delegation or, as applicable, the Information officer.
3. Confidential information^{42/} shall be labeled with the word "CONFIDENTIAL,"^{43/} which shall be placed in a spot visible to anyone who accesses it.

Article 40. Declaration of reserve

-
42. Comment: If the declaration of confidentiality covers the entire Document, there will be no need to identify its individual components. If only some of its component sections are classified as confidential, that circumstance shall be noted in the declaration of confidentiality.
 43. Comment: In any case, based on the type of confidential Information involved, the subject entities may establish special labeling systems the meaning of which is comprehensible only to those who have authorized access, making identification difficult for anyone else.

1. Information shall be classified as reserved on a case by case analysis, through the application of a harm test.
2. At the time the Information is classified, a resolution declaring the reserve must be issued, which indicates:
 - a) the subject entity that produced the Information;
 - b) the date or the event to which the reserve refers;
 - c) the authority that adopted the decision to reserve the Information;
 - d) persons authorized to access that Information;
 - e) distinction between the portions of the Information that are subject to confidentiality or reserve and those that are available for access by the public; and
 - f) the duration of the reserve.

Article 41. Declassification of Information

Information classified as reserved shall be public when:

- a) the causes that led to their classification cease to exist;
- b) the classification period expires;
- c) there is a resolution of the Guarantor Body or the judiciary that determines the existence of a public interest reason that prevails over the reserve of the Information; and
- d) the senior authority of the corresponding administrative unit of the subject entity considers declassification appropriate, in accordance with the provisions of this Law.

Article 42. Revision of the exceptions regime

The Guarantor Body shall periodically revise the list of exceptions established in this Law and recommend to the Legislative Branch the exclusion of those matters that no longer merit the nature of secret or confidential information or that for other reasons it feels should be excluded as grounds for secrecy or confidentiality.^{44/}

Article 43. Registry of classified Information

1. Subject entities shall, through their Information officers, submit to the Guarantor Body every six months an index of information classified as reserved or confidential.
2. The Guarantor Body shall publish that Information in open formats on the day following its receipt. Said index shall indicate the area that generated the Information, the name of the Document, the type of classification, whether a complete or partial classification is involved, the date when classification begins and ends, its justification and, as applicable, the sections of the Information that

44. Comment: this Information may be submitted in the annual report that the Guarantor Body presents to the Legislative Branch.

are classified and whether an extension is in effect. In no case may the index itself be considered as classified Information.

Article 44. Partial disclosure

In those circumstances in which not all the information in a Document is exempt from disclosure in accordance with the exemptions indicated in Article 33, an edited version of the Document must be prepared redacting only the portions of the Document that are subject to exception. The non-exempt Information shall be made public and delivered to the requester.

The subject entity shall make a note on the Document stating the reasons why certain Information has been suppressed.

Article 45. Maximum duration of reserve

1. The exceptions referred to in Article 303 are not applicable to a Document that is more than [5] years old. When a subject entity wants to reserve the Information, this duration may be extended for another [5 years] with the approval of the Guarantor Body. The duration of the reserve shall start on the date when the Information is first classified.^{45/}
2. Under exceptional circumstances, when in the judgment of the subject entity it is necessary to again extend the period of reserve of the Information, a duly founded and justified request shall be made to the corresponding Guarantor Body, applying the harm test and indicating the new period of reserve, at least three months prior to expiration of the original term.
3. Within no more than [7] business days, the Guarantor Body shall issue a resolution in which it may extend, modify or deny the requested period of reserve. The Information will continue to be reserved until the Guarantor Body makes a decision.
4. No type of Information may be reserved indefinitely.
5. In no event may the total period of secrecy exceed [10] years, including any extensions.

Article 46. Non-Existent Information

1. The subject entity may not refuse to deliver Information by unjustifiably alleging that it does not exist. The declaration that Information does not exist must always be proven and preceded by a properly documented search process in different administrative units.
2. The existence of Information is presumed when it pertains to the authority, duties and functions that the domestic legal framework grants to the subject entities, or to the commitments undertaken by the State at the international level.

45. Comment: The standard ISO15489 on Document management establishes that the assessment process falls to the producer of the information, which shall determine the period of secrecy of the Information.

3. Where certain powers, responsibilities or functions have not been exercised, the response must be justified based on the grounds supporting the inexistence of the Information.

4. If the requested Information is not found in the files because there is no obligation to generate it, this shall not be considered to mean that it doesn't exist but rather a lack of legal authority.

5. When declaring that the requested Information is inexistent, the subject entity shall assure the requester that it used an exhaustive search criterion, which it shall describe in its response to the requester, in addition to indicating the circumstances of time, manner and place that led to the inexistence of the Information.

6. The subject entity must duly prove the facts if the Information does not exist due to natural disasters, the commission of some crime, or if its elimination was authorized negligently or illegally. In all these cases, if the Information is of public interest, the subject entity shall do everything possible to reconstruct it.

7. The senior authority of the corresponding administrative unit shall be immediately informed of cases in which the institution for which it is responsible denies public Information by alleging the inexistence thereof, including the identification of the person or public official responsible for keeping the Information. The senior authority of the administrative unit shall in these cases:

- a) analyze the case and take the necessary measures to locate the Information;
- b) issue a resolution confirming that the Information does not exist;
- c) ensure, provided this is materially possible, that the Information is generated or replaced (when it should exist) to the extent possible based on its powers, responsibilities or functions. With prior verification of the inability to generate the Information, there should be a well-founded and reasoned exposition of the reasons why, in the specific case, it did not exercise those powers, responsibilities or functions, which shall be communicated to the requester; and
- d) immediately notify the supervisor of the subject entity and the Guarantor Body, the internal control body or the equivalent which, as applicable, shall initiate the administrative liability or other appropriate procedure.

8. The Guarantor Body is responsible for verifying that the information does not exist by means of:

- a) an on-site examination of the institutional files of the subject entity that declared the inexistence of the Information, to determine whether the Information search procedures were properly executed and confirm whether or not the Information actually exists;
- b) half-yearly requests to all subject entities of cases in which Information has been denied by alleging its inexistence. Said data shall be disclosed in the annual report referred to in Article 66; and
- c) requesting the responsible administrative unit to prepare a declaration of inexistence, in which the search actions are detailed.

Article 47. Filing of appeals

1. Anyone has the right to appeal the subject entity's decision not to deliver the requested Information by alleging one of the grounds contained in the exceptions regime.
2. This right includes the ability to challenge the declaration of reserve, made by a subject entity, before the Guarantor Body through the appeal procedure established in Chapter V of this Law.

Article 48. Recourse against a failure to respond

1. When the requester does not obtain a response in the established period, said requester may file a complaint with the Guarantor Body.
2. The complaint must be filed within [thirty] business days from the date in which a response should have been received by the requester; otherwise, the complaint may be rejected.
3. The Guarantor Body shall verify within a period of [five] business days whether the request for Information to the subject entity complies with the requirements of Article 12. If it does, the Governing Body shall admit the case and allow a period of [three] business days for the subject entity to justify the reasons why it did not provide a timely response to the request.
4. Once the period for the subject entity to justify its non-responsiveness has elapsed, the Guarantor Body shall verify, within [ten] business days, whether or not the requested Information is reserved or confidential. If the information is open for public access, the Guarantor Body shall issue a resolution ordering that the requester be given access to the Information.

Article 49. Other laws

The provisions on reserve or confidentiality of Information contained in other laws shall be consistent with the bases, principles and provisions established herein and may in no event contravene this Law.

In the event that other laws prescribe longer classification periods, those set forth in this Law shall prevail.

CHAPTER V. APPEALS

Article 50. Internal appeal^{46/}

1. A requester may file an internal appeal with the head of the Public Authority within [60] business days from the date in which the term for obtaining a response has expired, or from the date of any other breach of the rules set forth in this Law for responding to a request for Information.
2. The head of the Public Authority must issue a written and sufficiently reasoned decision within [10] business days from receipt of the notice of appeal, and deliver a copy of said decision to the requester.

46. Comment: An internal appeal should not be mandatory, but instead optional for the requester before proceeding to the external appeals process.

3. Should the requester decide to file an internal appeal, the full term for resolution thereof must expire before an external appeal may be pursued.

Article 51. External appeal

1. Any requester who believes that his or her request for Information has not been processed in accordance with the provisions of this Law, shall have the right to file an appeal with the Guarantor Body regardless of whether an internal appeal has been pursued.
2. Said appeal shall be filed within no more than [60] business days from the expiration of the terms for responding to a request for Information or to an internal appeal, as provided by this Law.
3. The request for an appeal shall contain:
 - a) the public authority with which the request was filed;
 - b) the contact information of the requester;
 - c) the grounds upon which the appeal is based; and
 - d) any other information that the requester considers relevant.
4. Upon receiving an appeal, the Guarantor Body may attempt to mediate between the parties with an aim to disclose the Information without exhausting a formal appeal process.
5. The Guarantor Body shall log the appeal in a centralized tracking system and inform all interested parties, including interested third parties, about the appeal and their right to participate in such process.
6. The Guarantor Body shall set clear and nondiscriminatory rules regarding the processing of appeals which ensure that all parties have an appropriate opportunity to appear in the process.
7. In the event the Guarantor Body is uncertain as to the scope and/or nature of a request and/or appeal, it must contact the appellant to clarify what is being requested and/or appealed.

Article 52. Resolution

1. The Guarantor Body shall decide appeals, including attempts to mediate, within [60] business days and may, in exceptional circumstances, extend this timeline by another [60] business days.
2. In deciding the case, the Guarantor Body may:
 - a) deny the appeal; or
 - b) require the Public authority to take such steps as may be necessary to comply with its obligations under this Law, such as, but not limited to, providing the Information and/or reducing the fee;

3. The Guarantor Body shall serve notice of its decision to the requester, the Public Authority and any interested party. Where the decision is unfavorable to the requester, the latter shall be informed of the right to appeal.

4. If a Public Authority does not comply with the Guarantor Body's decision within the time frame set forth in said decision, the Guarantor Body or the requester may file petition the [appropriate] court to compel compliance therewith^{47/}.

Article 53. Judicial review^{48/}

1. A requester may file a case with the court only to challenge a decision of the Guarantor Body, within [60] days of notice of the adverse decision or the expiration of the term for responses provided herein.

2. The court shall come to a final decision on all procedural and substantive aspects of the case as early as possible.

Article 54. Burden of Proof

1. The Public Authority shall have the burden of proof to establish that the requested Information is subject to one of the exceptions contained in Articles 32 and 33 above. In particular, the Public Authority must establish:

- a) that the exception is legitimate and strictly necessary in a democratic society based on the standards and jurisprudence of the Inter-American System;
- b) that disclosure of the Information would cause substantial harm to an interest protected by this Law; and
- c) that the likelihood and gravity of that harm outweighs the public interest in disclosure of the Information.

CHAPTER VI. GUARANTOR BODY

Article 55. Creation^{49/}

This Law creates a Guarantor Body that will promote and guarantee the right of access to public Information as well as the faithful implementation and interpretation of this Law.

47. Comment: The manner of enforcing the Guarantor Body's decisions in accordance with paragraph 4 will vary from country to country.

48. Comment: These rules are based on the assumption that in many countries courts have all of the inherent powers needed to process these types of cases, including for example imposing sanctions on Public Authorities. Where this is not the case, these powers may need to be explicitly given to them through the access to public Information law.

49. Note: Model Law 1.0 had an *Information Commission*; Model Law 2.0 considers it necessary to replace it with a newly created and more evolved *Guarantor Body*.

Article 56. Characteristics^{50/}

1. The Guarantor Body^{51/} shall be a body that has its own legal personality and is:
 - a) established by law.
 - b) autonomous and independent, with the ability to decide on the execution of its budget.
 - c) specialized and impartial.
 - d) authorized to impose penalties, within its areas of competence.

Article 57. Composition

1. The Guarantor Body shall be composed of (five or more) commissioners.^{52/}
2. The Guarantor Body should reflect a diversity of experience and talent, as well as gender parity.

Article 58. Requirements to be a commissioner

Commissioners must meet the following minimum requirements:

- a) be a citizen in full possession of the inherent political and civil rights;
- b) have knowledge and proven experience in the field covered by this Law, in order to ensure independent judgment and impartiality;
- c) have a good reputation, not have been convicted of a crime involving fraud or dishonesty in the past five years, and not have been convicted of corrupt acts as defined in the Inter-American Convention against Corruption and under domestic law.

Article 59. Selection procedure

50. Note: unlike Model Law 1.0, an article is created detailing the essential and non-essential characteristics with which the Guarantor Body must be created.

51. Comment: Each State may consider the Guarantor Body to be preferably:

- i) established at the constitutional level;
- ii) not subordinated to any branch, body, or institution of government;
- iii) collegiate, or with accountability mechanisms;
- iv) independent of local transparency bodies, in the case of Federal States.

52. Comment: It is preferable that Guarantor Bodies be composed of an odd number of commissioners greater than or equal to five (5), since a body composed of three (3) may isolate or obstruct the opinion and participation of one of the commissioners in cases where the other two are closely aligned philosophically, personally, or politically—a dynamic that is less likely to arise in a collegial body of five or more members.

Each State may consider the possibility of selecting alternate commissioners. Alternate commissioners may be those who, while not having been chosen during the selection process, have nonetheless obtained the best scores. In any case, it must be ensured that the absence/vacancy of a commissioner does not hinder the operation of the Guarantor Body.

Commissioners shall be nominated by a majority of [two-thirds] of the members of the [Legislative Branch] and appointed by the [Executive Branch], in a process that adheres to the following principles:

- a) public participation in the nomination process;
- b) transparency and openness; and
- c) publicity of the list of candidates considered most suitable for the position.^{53/}

Article 60. Obligations of commissioners

- 1. Commissioners shall perform their duties on a full-time basis.
- 2. Commissioners may not hold any other employment, position, or commission except in academic, scientific, or philanthropic institutions.^{54/}

Article 61. Term of office

- 1. The term of office of the commissioners shall be [5] years, renewable for a single additional term.
- 2. The election of commissioners must be alternated and held at staggered intervals, in order to prevent the mandate of more than two thirds of its members from expiring in the same year and to ensure the continuity of service, as well as to guarantee the autonomy and political independence of the Guarantor Body.
- 3. Commissioners shall remain in office until their replacements are elected.^{55/}

Article 62. Removal or suspension of commissioners

- 1. Commissioners may only be removed or suspended from office following a process that is similar in nature to that by which they were appointed or for a situation that warrants removal from office, including:
 - a) a final judgment of conviction for a criminal offense or punishment for violating ethical

53. Comment: In order to increase confidence in the institution, it is preferable that both the Executive and the Legislative Branches participate in the selection process; that any decision of the Legislative Branch be adopted by a qualified majority sufficient to guarantee bipartisan or multi-partisan support (e.g., 60 percent or 2/3); that the public and civil society have the opportunity to participate in the nomination process; and that the process be transparent. There are two main approaches: appointment by the Executive Branch, with the nomination and approval of the Legislative Branch; and appointment by the Legislative Branch, with the nomination or approval of the Executive Branch.

54. Comment: It is recommended that commissioners serve on a full-time basis and that their salary be tied to an externally fixed sum in order to strengthen their independence.

55. Comment: It is recommended that commissioners hold office for no longer than 12 years, including any re-election.

standards of conduct;

- b) infirmity that directly affects the individual's capacity to discharge his or her duties;
- c) serious constitutional violations or breaches of this Law, or the mismanagement of Public Funds and resources;
- d) refusal to comply with any of the disclosure requirements inherent to their position, such as the public disclosure of salary or benefits; and
- e) negligent or bad faith disclosure or use of sensitive or confidential Information.

2. Any commissioner who has been removed or suspended from office has the right to appeal such removal or suspension to the Judicial Branch.

Article 63. Duties and powers of the Guarantor Body^{56/}

The Guarantor Body shall have all the powers necessary to perform the functions described in this Law, including the following:

I. Interpretation of the Law:

- a) interpret this Law and ensure that its correct interpretation by subject entities.

II. Implementation of the law:

- a) monitor and ensure *ex officio* compliance with this Law;
- b) support Public Authorities in the implementation of this Law; and
- c) implement a set of indicators to measure the proper application of this Law.

III. Regulations:

- a) propose legislative initiatives in the area of its competence;
- b) make recommendations on existing and proposed legislation in the area of its competence;
- c) propose, coordinate, or, where appropriate, approve the Regulations to the Law on Access to Public Information and the internal rules necessary for the proper performance of its duties, including the design of its organizational structure; and
- d) draft guidelines for the handling of public, confidential, and classified Information in the possession of subject entities.

IV. Information asset registers:

- a) keep a record of requests for access to Information, responses, results, and costs of reproduction and delivery.

V. Direct internal policies:

56. Note: Unlike Model Law 1.0, Model Law 2.0 includes a list detailing the duties and powers of the Guarantor Body.

- a) provide guidance to subject entities in the design, implementation, and assessment of actions to disseminate public Information; and
- b) promote the homogeneity and standardization of Information disseminated by the subject entities, through the adoption of guidelines, templates, and any means deemed appropriate.

VI. Digitalization of Information and information and communication technologies:

- a) promote and guide the digitalization of public Information in the possession of subject entities as well as the use of modern and adaptable information and communication technologies.

VII. Open data:

- a) ensure that key Information is increasingly disclosed in an open data format; and
- b) provide technical support to reporting entities in the preparation and dissemination of Information in an open data format.

VIII. Orders:

- a) issue binding decisions and orders; and
- b) disclose the orders issued, particularly among the subject entities, in order to standardize the enforcement of this Law.

IX. Requests for Information:

- a) promote the development and implementation by the subject entities of a modern computer system for the intake of requests through a single window; and
- b) prepare forms for the submission of requests for information, which are not binding but will serve as a general guide for regulated entities and will contain the requirements established in [Article 23 of Law 1.0].

X. Dispute resolution:

- a) resolve disputes relating to the classification and declassification of classified or confidential information, applying the principle of maximum openness; and
- b) create and offer free and expeditious mechanisms for the resolution of disputes that may arise between subject entities and Information requesters, and mediate and/or adjudicate such disputes.

XI. National security:

- a) request the cooperation of institutions in the national security and defense sector to obtain technical inputs to ensure the appropriate declassification of Information.

XII. Inspections and investigations:

- a) in the context of a proceeding, to summon individuals, request searches, and receive the sworn testimony of persons deemed to be in possession of Information relevant to the performance of their functions;

- b) verify and review public Information in the possession of any subject entity, through on-site inspections. This Information may include classified or confidential Information;
- c) these proceedings include, *inter alia*, the supervision and observation of the request intake system of the subject entities in order to verify that they adequately respond to requests for Information; and
- d) issue the appropriate preventive/precautionary measures by means of a reasoned order, *inter alia*, to request a copy of the Information in dispute, regardless of its classification; notify the offender's supervisor of the alleged conduct and the existence of the proceeding before the Guarantor Body; and request that the head of the regulated entity take special measures to safeguard and back up the Information in question.

XIII. Compliance lists:

- a) adopt the necessary guidelines for monitoring compliance with this Law, including the periodic publication of the list of subject entities that comply/fail to comply with the provisions of this Law, including the incorporation of a gender perspective; and
- c) publish a list identifying the subject entities against which the highest number of complaints was received.

XIV. Reports of violations:

- a) refer cases of suspected administrative or criminal misconduct to the competent bodies.

XV. Penalties and enforcement measures:

- a) establish and carry out enforcement measures, including public and private reprimands, fines, and others.

XVI. Legal Recourse:

- a) serve as a second instance for persons who are dissatisfied with the resolutions of the subject entities;
- b) in the case of Federated States, serve as a second instance in the event of denial by local bodies;
- c) resolve individual complaints, which may be filed at any time under the legally established guidelines and procedures;
- d) hold oral and public hearings to determine the classification or declassification of Information, as appropriate;
- e) call witnesses and produce evidence in the context of an appeal; and
- f) as the result of an appeal, the Guarantor Body may, *inter alia*, order the declassification of Information and consequently its release.

XVII. Training:

- a) promote and implement training and awareness programs directed at subject entities, in particular public servants, and provide any technical support they may require on matters within their competence.

XVIII. Public awareness:

- a) hold workshops, conferences, seminars, and other similar activities to publicize the importance of the right of access to public Information as a tool to ensure transparency;
- b) sign cooperation agreements with all kinds of public and private organizations that promote access to public Information; and
- c) disseminate this Law and promote its understanding among the general public through the publication and dissemination of guides and other similar resources on the relevance of the right of access to Information and its practical application, taking into account accessibility criteria for groups in situations of vulnerability.

XIX. Constitutional challenges:

- a) bring unconstitutionality actions in matters within its competence to challenge federal or state laws as well as international treaties signed by the Executive Branch and ratified by the Legislative Branch that violate the right of access to public Information.

XX) International conventions:

- a) ensure compliance with the obligations undertaken by the State in international conventions, specifically regarding access to public Information, including the Inter-American Convention against Corruption and the United Nations Convention against Corruption.

XXI. Coordination with national archives:

- a) cooperate with the entity in charge of the national archives in the creation and use of the criteria for cataloguing and conserving Documents, in the organization of the archives of the agencies and entities subject to this Law, as well as in other areas of mutual interest.

Article 64. Budget^{57/}

1. The Legislative Branch must approve the budget of the Guarantor Body, which must be sufficient for it to properly discharge its duties.
2. The creation of new bodies shall guarantee the provision of sufficient human, budgetary, and material resources for them to perform their duties, as this is the only way to guarantee sufficient conditions for the proper application of this Law.

Article 65. Reports of subject entities^{58/}

1. Subject entities shall submit annual reports to the Guarantor Body detailing the activities they carry out to comply with this Law. This report shall include, at a minimum, information on:
 - a) number of requests for Information received, granted in whole or in part, and of requests denied, disaggregated by gender where possible, as well as any other Information related to indigenous groups, economically disadvantaged persons, women, persons with disabilities, Afro-descendants, and others, for purposes of evaluating the implementation of this Law. In

57. Note: Model Law 2.0 introduces a specific article on the budget of the Guarantor Body.

58. Note: Model Law 2.0 details the information that both the report of the Guarantor Body and the report of the subject entities should contain.

order to collect this Information, reporting entities may use Information request forms^{59/} with minimum fields to be completed by the requesters;

- b) number of requests responded extemporaneously, including justification for any delay;
- c) details of the sections of this Law that were invoked to deny, in whole or in part, requests for Information and the frequency with which they were invoked;
- d) response time to requests for Information;
- e) number of appeals filed to contest the denial of Information, disaggregated by gender;
- f) fees charged for the reproduction and delivery of the requested Information;
- g) activities undertaken to meet the obligation to disclose key Information and those undertaken to implement the open State policy;
- h) activities carried out to implement proper document management;
- i) activities to provide training and education to public servants; and
- j) gender-disaggregated statistics and information demonstrating compliance with this Law.
- k) difficulties observed in complying with the Law.

2. The Guarantor Body may gradually expand the above list as it deems advisable to verify compliance by the subject entities with the provisions of this Law. To this end, the Guarantor Body will issue the guidelines it deems necessary.

Article 66. Reports of the Guarantor Body

The Guarantor Body shall publish annual reports on its activities and on the implementation of the Law. Said report shall include at least the following:

- a) a systematized summary of the Information received from subject entities in compliance with this Law;
- b) the number of appeals filed, disaggregated by gendered including those from the various public authorities, their grounds, results, and status;
- c) number of penalty proceedings filed and their current status;
- d) list of public servants penalized for failure to comply with this Law; and
- e) disaggregated statistical Information that makes it possible to identify and define inequalities that require the adoption of differentiated measures and the measures and proposals that will be undertaken in order to narrow the gaps between different sectors of society. Criminal and Civil Responsibility

Article 67. Civil and criminal liability

59. Comment: The omission of the requirement to complete the information request forms shall not be grounds for invalidating such request.

1. No one shall be subjected to civil or criminal action, or to any employment detriment, for any action taken in good faith in the exercise, performance or purported performance of any power or duty in terms of this Law, as long as they acted reasonably and in good faith.
2. It is a criminal offense to willfully destroy or alter Documents after they have been the subject of a request for Information.

Article 68. Administrative offenses

1. It is an administrative offense to willfully:
 - a) obstruct access to any Document in contravention of Chapter II of this Law;
 - b) prevent the performance by a Public Authority of its duty under Chapters II and III of this Law;
 - c) interfere with the work of the Guarantor Body;
 - d) fail to comply with provisions of this Law;
 - e) fail to create a Document either in breach of applicable regulations and policies or with the intent to obstruct access to Information; and
 - f) destroy Document without authorization.
2. Anyone may make a complaint about an administrative offense as defined above.
3. Administrative sanctions shall be governed by the administrative law of the State and may include a fine [of up to x times the minimum wage], a suspension of a period for [x] months/years, termination, or a separation or restriction from service for [x] months/years].
4. Any sanctions ordered shall be posted on the website of the Guarantor Body and the respective Public Authority within five days of the imposition thereof.

CHAPTER VII. PROMOTIONAL AND COMPLIANCE MEASURES

Article 69. Monitoring and compliance

1. The [legislative body] should regularly monitor the operation of this Law, in order to determine whether changes and improvements are necessary to ensure all Public Authorities comply with the text and spirit of the Law, and to ensure that the government is transparent, remains open and accessible to its citizens, and guarantee the fundamental right of access to Information.

Article 70. Training

1. The Information Officer shall ensure the provision of appropriate training for the officials of the Public Authority on the application of this Law.
2. The guarantor Body shall assist Public Authorities in providing training to officials on the application of this law.

Article 71. Formal Education

1. The [Ministry of Education] shall ensure that core education modules on the right to Information are provided to students in each year of primary and secondary education.

CHAPTER VIII. TRANSITORY PROVISIONS

Article 72. Abbreviated title and entry into force

1. This Law may be cited as the Access to Public Information Law of [year].
2. This Law shall be effective on the date of its promulgation by [insert name of relevant official such as President, Prime Minister], regardless of which it shall become effective automatically [six] months after its approval in the absence of a promulgation.
3. The Guarantor Body shall have up to 6 months from the date in which this Law becomes effective to appoint its personnel, establish its internal processes, disseminate information proactively and carry out any other action needed for its full operation.

Article 73. Regulations

1. This Law must be properly regulated within [1] year of its entry into force, with active involvement of the Guarantor Body.
