PERMANENT COUNCIL OF THE
ORGANIZATION OF AMERICAN STATES

COMMITTEE ON JURIDICAL AND POLITICAL AFFAIRS

OEA/Ser.G
CP/CAJP-2921/10
19 November 2010
Original: English

DRAFT:
PRELIMINARY PRINCIPLES AND RECOMMENDATIONS ON DATA PROTECTION (THE PROTECTION OF PERSONAL DATA)

[Document presented by the Department of International Law, of the Secretariat for Legal Affairs, pursuant to, operative paragraph 11 of, General Assembly Resolution AG/RES. 2514 (XXXIX-O/09)]

DRAFT:
PRELIMINARY PRINCIPLES AND RECOMMENDATIONS ON DATA PROTECTION
(THE PROTECTION OF PERSONAL DATA)

-- Table of Contents --

DRAFT
PRELIMINARY PRINCIPLES AND RECOMMENDATIONS ON DATA PROTECTION (THE PROTECTION OF PERSONAL DATA)

[Document presented by the Department of International Law, of the Secretariat for Legal Affairs, pursuant to operative paragraph 11 of General Assembly Resolution AG/RES. 2514 (XXXIX-O/09)]

I. INTRODUCTION

Procedural Background

The General Assembly of the Organization of American States, since 1996, has expressed special attention to matters concerning access to information and protection of personal data and, via resolution AG/RES. 1395 (XXVI-O/96), requested the Inter-American Juridical Committee begin to study the legal frameworks of OAS member States related to these two topics. On the topic of Access to Public Information, the General Assembly requested additional work from the Member States and the organs, organisms and entities of the OAS via subsequent resolutions AG/RES. 2057 (XXXIVO/04), AG/RES. 2121 (XXXV-O/05), AG/RES. 2252 (XXXVI-O/06), AG/RES. 2288 (XXXVIIO/07), AG/RES. 2418 (XXXVIII-O/08) and AG/RES. 2514 (XXXIX-O/09). This work culminated in the adoption of AG/RES. 2607 (XL-O/10), in June of 2010, with the text of a Model Inter-American Law on Access to Public Information, which also instructed the General Secretariat to provide support to the member states in the design, execution, and evaluation of their local legal frameworks regarding access to public information.

On the topic of the protection of personal data, the General Assembly has requested several studies and documents from the Inter-American Juridical Committee on access/protection of information and personal data, including OEA/Ser.Q CJI/doc. 52/98, CJI/doc.25/00 rev.1, CJI/doc.162/04, CJI/doc.232/06 rev.1, CJI/doc.25/00 rev.2 of 2007 and CJI/doc.239/07. The Inter-American Juridical Committee also adopted several resolutions on this matter, including CJI/RES.9/LV/99, CJI/RES.33 (LIX-O/01), CJI/RES.81 (LXV-O/04), and CJI/RES.130 (LXXI-O/07) all in an effort to address the regulation of data protection through potential international instruments as well as at the level of the legislation of some OAS member states, and of the processing of personal data by the private sector. This work provided valuable input not only to understand the true dimension of this issue in the light of the impact that new technologies have on the expansion of the manipulation and use of the information by individuals, but to help States to take actions regarding law harmonization, improved regional cooperation and finding substantial elements for a future regional instrument on the matter.

In addition to the work of the Inter-American Juridical Committee, the General Assembly, via resolutions AG/RES. 2288 (XXXVIIO/07), AG/RES. 2418 (XXXVIII-O/08) and AG/RES. 2514 (XXXIX-O/09), requested that the General Secretariat prepare the draft preliminary study contained herein, the intent of which is merely to provide a comparative look at the most prevalent systems for data protection, that OAS member states may take into account in drafting principles and recommendations, and in considering international instruments and national legislations on the topic.

Substantive Background

The Inter-American Juridical Committee explained in its Annual Report to the General Assembly in 2007 that advances in computer technology, medicine and biotechnology there has been a marked increase in the processing of personal data in the various spheres of economic and social activity. The progress made in information technology also makes the processing and exchange of such data across international borders relatively easy. The challenge, therefore, is to protect fundamental rights and

freedoms, notably the right to privacy and the right to access personal information (also known as habeas data), while encouraging the flow of information and electronic commerce.

In this regard, it is well accepted that the use of electronic systems for collecting, storing, transferring and disseminating personal information grows exponentially each year. As a result, the quantity and types of personal information available on individuals has caused concern for some privacy advocates. And although it is difficult to ascertain what personal data is (privately or publicly) available -- a problem compounded by the wide array of governmental and non-governmental actors in custody of personal information -- many advocate for new methods of regulating how the information is collected and how it is used. These calls frequently focus on the lag between technology and regulation; the former of which has evolved at a very rapid speed, while the latter has advanced at a much slower pace.

Legislation on data protection is based on an individual's right to privacy. However, the meaning of privacy and the origins of an individual's right to privacy can vary. As a result, policies and laws governing the right to privacy differ from country to country. Because of this divergence in the treatment of the right to privacy, legislation protecting the treatment of personal data can vary between regions. Generally speaking, the treatment of data protection has followed one of three approaches. The European system is the strictest current system of government-regulations with legislation governing both the collection of personal data by the government and private organizations. The United States' follows a bifurcated approach, which allows industry regulation of personal data collected by private organizations and government regulation of data collected by the government. Finally, several Latin American countries have developed data protection mechanisms based on the concept of *Habeas Data*, which allows individuals access to their own personal data and the right to correct any mistaken information.

A new approach by Mexico, which became the first Latin American country to undertake comprehensive reform in this field, attempts to bridge these various approaches. The new federal Law for the Protection of Personal Data, which entered into force in July 2010, combines some self-regulatory features, with the ability to correct mistaken data, and statutory oversight. As will be detailed further below, despite these different approaches in the regulation of personal data, there are some fundamental principles that have served as the basis for data protection legislation throughout the world.

Because of the marked difference in the treatment of the right to privacy and data protection in Europe and the United States, part one of this paper will provide a brief overview on the right to privacy and data protection in Europe and in the United States. Part two will discuss *Habeas Data* and its role in the protection of personal data. Part three will discuss definitions that are fundamental to the protection of personal data. Part four will then detail fifteen principles that are the basis for data protection legislation worldwide and which could serve as the basis for an international instrument or model law on data protection. Each fundamental section will also include recommendations for each principle. Part five of this paper will conclude with proactive measures Organization of American States ("OAS") member states can undertake to protect personal data and foster cooperation among national and international authorities.

II. DATA PROTECTION IN EUROPE AND UNITED STATES

The Council of Europe ("COE") recognizes the right to privacy as a "fundamental human right."[1] In addition, the *Universal Declaration of Human Rights* and the *United Nations International Covenant on Civil and Political Rights* both define privacy as the right to not "be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon [an individual's] honour and reputation."[2] Both agreements go on to explain that "everyone has the right to the protection of the law against such interference or attacks."[3]

As a result, the European view to the right to privacy covers every aspect of the individual's life. Based on this expansive view to the right to privacy, privacy legislation in Europe covers both the processing of personal data by the government and private organizations.[4] The COE's *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* ("Convention") broadly defines personal data as "any information relating to an identified or identifiable individual" and outlined data protection principles, which have served as the basis for data protection legislation worldwide. [5] Later, the European Union's *Data Protection Directive* ("Directive") affirmed the Convention's data protection principles, set the standard level of data protection for members of the European Union, and, more importantly, acknowledged the individual's right to privacy.[6] Because of this expansive concern over an individual's right to privacy, the Directive goes on to restrict the transfer of personal data to countries outside the European Union only if the country ensures "an adequate level of [data] protection."[7] In this way, the Directive extends the reach of protection afforded to personal data originating in the European Union to countries outside its borders. The Directive's has extended past EU borders, influencing data protection regulation worldwide by forcing other countries with companies interested in transferring personal data to examine their own data protection legislation and, if necessary, to change their legislation to meet the European Union's standards.[8]

In the United States, the right to privacy can be traced to the United States Constitution ("Constitution") and to common law.[9] In one of the most influential American articles on the right to privacy, the authors argued that privacy was "the right to be let alone."[10] Since then, the United States Supreme Court ("Court") has ruled in favor of privacy interests by deriving the right to privacy from the Constitution.[11] In its decisions, the Court has stated that the Constitution protects "the individual interest in avoiding disclosure of personal matters" and "the interest in independence in making certain kinds of important decisions."[12] However, the Court has also held that the right to privacy was not absolute and an individual's privacy interest must be balanced against "competing public interests."[13]

The right to privacy in the United States, unlike the European approach, protects only against the federal government's intrusion into an individual's private affairs. Hence, the legislation specific to the issue of personal data protection is limited to data processed by and in custody of the federal government.[14] Other than a few laws dealing with personal financial and medical information, the United States does not have legislation that governs the processing of personal data by private organizations.[15] Instead, the U.S. system provides for self-regulation by industry of the personal data handled by private organizations. As such, industries in the United States are mostly self-regulated, including most private corporations, data-mining businesses, personal data repositories and internet-based social-networking sites, among others.

For cases in which private parties which to comply with predetermined guidelines on the handling of personal data, the U.S. Federal Trade Commission ("FTC") has developed a safe harbor provision which certifies that the organization in question provides an adequate level of protection to personal data.[16] Although this provision is voluntary in the domestic context, companies that receive personal data from members of the European Union must employ these guidelines for the cross-border handling of information. In addition, the fact that United States legislation focuses exclusively on protecting individual information processed by the federal government, the level of protection afforded to personal data processed by private organizations in the United States and then transferred to an another country remains unclear.[17]

III. DATA PROTECTION IN LATIN AMERICA

Habeas Data

Habeas Data literally means "you should have the data."[18] Although its origins can be traced to Europe, in Latin America *Habeas Data* is a complaint presented to a court, which allows for the protection of an individual's "image, privacy, honor, information self-determination, and freedom of information."[19] *Habeas Data* is a mechanism that provides the individual with the power to stop abuse of the individual's personal data.[20] In general, *Habeas Data* provides an individual with access to personal information in public and/or private databases, the ability to correct or update the data, the ability to ensure that sensitive data remains confidential, and allows the removal of sensitive personal data, which may damage the individual's right to privacy.[21] Unlike data protection laws in Europe and in the United States, *Habeas Data* does not require private and public entities to proactively protect the personal data that they process. *Habeas Data* only requires that the aggrieved individual, after a complaint is presented to a court, is given access and the ability to rectify any personal data that may injure the individual's right to privacy.[22] Further, *Habeas Data* is reserved as a legal recourse only for individuals "whose privacy is being compromised."[23] Moreover, *Habeas Data* may not provide legal recourse to an aggrieved individual if the individual's personal data has been transferred outside the country.[24] As a result, the protection that *Habeas Data* provides is more limited than those provided by the European model. Some countries, like Argentina for example, have passed personal data protection legislation that supplements *Habeas Data* legislation already in place.[25]

Mexican Law

Mexico adopted a new Federal Law on the Protection of Personal Data in July 2010. Unlike the U.S. approach, which principally regulates data processing by public agencies, the new Mexican law regulates processing of personal data exclusively by private sector parties. Moreover, the Federal Institute for Access to Information, which prior to the enactment of the new Law on Personal Data had oversight exclusively over access to information in custody of government agencies, now has expanded powers to include private sector oversight when dealing with personal data -- even though the new law paradoxically does not apply to personal data processed by government agencies. Although there are questions related to the operation of the new Mexican law, it marks an important development in privacy and data protection laws in the Americas and, along with the E.U., U.S. and Habeas Data regimes provides a wealth of principles and rules to help regulate this important issue within OAS member states.

IV. DEFINITIONS

For purposes of this document, it is important to clearly define basic concepts relating to personal data protection because definitions may later affect other issues, such as who has standing to present a complaint alleging a violation of data protection laws to a court, and the scope of data protection laws. The following are some concepts whose definitions should be carefully considered.

Personal Data

The Convention and the Organization for Economic Cooperation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ("Guidelines") broadly define "personal data" as "any information relating to an identified or identifiable individual."[26] Hence, the Guidelines and the Convention could be applied to the personal data of natural and legal persons. Some countries recognizing the ambiguity tried to provide more clear definitions. For instance, *The Madrid Resolution* says that "personal data" means "any information relating to an identified natural person or a person who may be identified by means reasonably likely to be used."[27] Therefore, the Madrid Resolution extended its protection to all personal data that could be linked to an individual. On the other hand, Argentina's data protection act defines personal data as "information of any kind referred to certain or ascertainable physical persons or legal entities."[28] Argentina's legislation provides protection to the personal data of public and private entities. However, the United Kingdom's data protection act for

example, explicitly states that "personal data means data which relate to a living individual who can be defined."[29] By its own definition, the United Kingdom's data protection act does not extend to individuals that have died. However, if left ambiguous, data protection laws could be extended to protect the personal data of individuals after death. Personal data should clearly be defined because this definition may affect whose data is being protected, who may later allege data protection violations, and possibly limit the time that the individual's data is protected.

Data Controller and Data Processor

The Guidelines broadly define "data controller" as the "natural or legal person, public authority, agency or any other body who is competent according to national law to decide the purpose of the automated data file."[30] The Convention also broadly defines "data controller" to include "a party who, according to domestic law, is competent to decide … use of personal data."[31] Consequently, the Guidelines and the Convention apply to both public and private entities that deal with personal data. Yet, Australia and Canada, which have separate legislation for data processed by government and private organizations, clearly define the data controller depending on the legislation.[32] Further, the United Kingdom and Spain differentiate between a "data controller" and a "data processor."[33] In the United Kingdom and in Spain, a data processor processes the data on behalf of the data controller.[34] In effect, the data processor acts as an agent on behalf of the data controller.[35] For that reason, the data controller remains responsible for ensuring that all personal data processed by a data processor on their behalf complies with the law.[36] "Data controller" as opposed to simply a "data processor" should be clearly defined because this definition will dictate who is ultimately responsible with complying with data protection laws.

Sensitive Personal Data

The United Kingdom and Spain are among countries whose data protection acts defined "sensitive personal data" as consisting of information on racial or ethnic origin, political views, religion, union activities, physical or mental health, sexual preferences, and criminal history.[37] The categories of data that are considered sensitive should be clearly defined because sensitive data may require special treatment such as explicit consent for disclosure or there may a prohibition against processing this type of data unless there is a legal exception.

Processing

The Convention defines "automatic processing" as the "storage, carrying out of logical and/or arithmetical operations … alteration, erasure, retrieval, or dissemination.[38] The United Kingdom removed the "automatic" from its definition and then went on to define "processing" by describing almost every imaginable use of data by a data controller.[39] *The Madrid Resolution* opted for a very broad, but ambiguous definition of processing to cover almost every possible use of personal data.[40] *The Madrid Resolution* also states that it applies to "any processing of personal data, wholly or partly by automatic means, or otherwise in a structured manner, and carried out in the public or private sector."[41] Australia did not use the word "processing," opting instead for "use."[42] Australia defined "use" as the "handling of personal information within an organization."[43] Data processing should be defined broadly and, perhaps, in this instance, it may be useful to leave the definition ambiguous to ensure that the widest possible uses, including collection, of personal data are protected under the law. However, like the *Madrid Resolution*, it may be necessary to limit the definition of data processing to exclude the "processing of personal data by natural persons … related exclusively to his/her private and family life" so it is clear that data protection legislation is not intended to apply to individuals who may process personal data during the course of their private activities.[44] It may also be necessary to exempt law enforcement agencies, acting under legal authority and in very limited circumstances as authorized by national law, from complying with personal data protection legislation.[45]

Consent

The individual must adequately consent to the processing of the individual's personal data. The consent given by the individual should be defined as a "freely given specific and informed indication" of the individual's agreement to the processing of the individual's personal data.[46] However, when defining consent, the failure to respond to a data controller's request to process the individual's data should not be inferred to be consent from the individual.[47] Further, in the definition of consent, it should include the ability to withdraw consent and limit the amount of time that the consent is valid.[48]

More generally, the data controller should provide simple procedures for the individual to quickly and thoroughly withdraw consent.[49] In addition, an assessment of whether consent is valid may depend on the age, mental capacity, and the surrounding circumstances of when consent was given to the data controller to process the personal data.[50] Third party consent, such as that of a parent or guardian, may be needed when the individual is unable to provide adequate consent.[51] Adequate consent may be implicit or explicit. However, when dealing with sensitive personal data, consent should be explicit.[52] This means that the individual must unambiguously indicate the individual's agreement to the processing of the individual's personal data.[53]

V. PRINCIPLES AND RECOMMENDATIONS

The following principles have served as a basis for data protection legislation. The principles, some of which are interrelated, also include legal recommendations, which explain each principle.

Principle 1: Lawfulness and Fairness

Personal data should be processed lawfully and fairly. However, lawfully and fairly, as concepts, should be examined separately.

Lawfulness

The processing of personal data should be lawful. If the processing of personal data entails committing a criminal offense or could result in a lawsuit, then the processing may not be lawful.[54] In addition, unlawful processing of personal data may also involve a breach of a duty such as confidence, a contractual obligation, or international human rights legislation.[55]

Fairness

The processing of personal data should be fair. The *Madrid Resolution* states that "any processing of personal data that gives rise to … discrimination against" the individual is unfair.[56] For personal data processing to be fair there should be a legitimate reason for "collecting and using the personal data."[57] Personal data processing should not have "unjustified adverse effects on the individual concerned."[58] Personal data processing should be a transparent process. A transparent process includes notice to the individual of who is processing the individual's personal data, if the data will be shared with others, and its intended use.[59] Further, personal data should be processed only in ways that the individual "would reasonably expect."[60] If over time the use of the personal data changes into ways that the individual would not reasonably expect, then it may be unfair to use the personal data in such a way. At this point, it may be appropriate to seek the individual's consent for continued processing of the personal data.[61]

Principle 2: Specific Purpose

Personal data should be processed for a "specific, explicit, and legitimate purpose."[62] This means that from the outset, the purpose for the processing of personal data should be unambiguous.[63] This also means that the purpose of the processing of personal data should be aligned with the reasonable expectations of the individual at the time that the data was obtained or consent given.[64] Further, if sensitive personal data is being processed, then explicit consent from the individual should be required.[65] If the personal data is going to be processed for a purpose that is incompatible with the purposes for which it was obtained, then the individual's unambiguous consent is needed.[66] To determine if a new purpose or disclosure is compatible with the original purpose for which the data was obtained, it may be necessary to analyze whether the new intended use of the personal data is fair and lawful.[67] In the alternative, it may be necessary to determine if the new purpose arose from the context of the primary purpose to figure out if both the new and the primary purposes are related.[68] Furthermore, if sensitive personal data is involved, then the new purpose must be "directly related" to the primary purpose.[69]

Principle 3: Limited and Necessary

The personal data that is processed should be limited to that personal data necessary to achieve a specific purpose.

Limited

The processing of personal data should be limited. That means that the processing should be "adequate, relevant, and not excessive in relation to the purposes" for which the personal data was obtained.[70] The processing of the personal data should also be limited to the current reason for processing it.[71] This means that only the "minimum amount of personal data" to properly fulfill the purpose should be processed.[72] However, the amount of personal data should be sufficient to fulfill the specific purpose for which the data was obtained and processed.[73] Additionally, personal data should not be "disclosed, made available, or otherwise used for purposes" other than the specific purposes for which it was originally obtained and processed, unless the individual consents or by legal authority.[74]

Necessary

Reasonable efforts should be made to limit the processing of personal data to the minimum necessary.[75] If the personal data is required to "effectively pursue a legitimate function or activity," then the processing of that personal data should be necessary.[76] More specifically, the processing of personal data is only necessary if it "directly helps to achieve" the purpose for which it was obtained and processed.[77] If the purpose can be achieved through another reasonable means, then the processing of the personal data is not necessary.[78] The following are some conditions that may make the processing of personal data necessary: 1) entering or performing a contract; 2) complying with a legal obligation; 3) protecting the interests of the individual; 4) pursuing the interest of justice; and 5) protecting the legitimate interests of the data controller unless it prejudices or harms the interests of the individual.[79] Moreover, while it should not be permissible to process personal data that may be "useful in the future," it may be necessary to process personal data "for a foreseeable event that may never occur."[80]

Principle 4: Transparency

It is important for the processing of personal data to be a transparent process. Transparency in the processing of personal data is especially important if the individual has a choice as to whether to enter into a relationship with the data controller.[81] The following help ensure transparency in the processing of personal data.

Information about the Data Controller

When processing personal data, the data controller at a minimum should provide the following information about the data controller to the individual: 1) information about the data controller's identity; 2) the intended purpose of the personal data processing; 3) to whom the personal data may be disclosed; 4) how the individual's may exercise any rights afforded by data protection legislation; and 5) any other information necessary for the fair processing of the personal data.[82] If appropriate, the data controller should disclose the legal authority that authorizes the data controller to process the personal data.[83] Since it may later affect issues of jurisdiction and choice of law, it is important to include the identity of the local data controller's representative if the data controller is located in a third country.[84]

When to Disclose Information about the Data Controller

If the personal data was collected directly from the individual, then information about the data controller and the purpose of the data processing should be "provided at the time of collection," if the information has not already been provided.[85] If the personal data of the individual was obtained from a third party, then the data controller must inform the individual about the source of the personal data.[86] The information should be provided within a "reasonable period of time." However, if compliance is unfeasible or it involves a disproportionate effort by the data controller, then alternate methods to inform the individual may be used.[87]

How to Disclose Information Involving Personal Data Processing

Information should be provided to the individual in an "intelligible form, using clear and plain language."[88] All information should be decoded and if necessary, explanations should be included.[89] An average person should be able to understand the information.[90] It may be necessary to translate the information into another language or to take into consideration the special needs of minors when providing information regarding personal data processing.[91]

Principle 5: Accountability

The data controller is responsible for taking all the necessary steps to follow personal data processing measures imposed by national legislation and other applicable authority.[92] In addition, the responsibility lies with the data controller to show individuals and the appropriate supervisory authority that the data controller is complying with necessary measures, as established by national legislation or other authority, to protect the individual's personal data.[93] The latter should include how the data controller manages requests for access to personal data information and what kind of personal information the data controller processes.[94]

Principle 6: Conditions for Processing

The processing of personal data should only take place if one of the following conditions exists and the processing is fair and lawful.[95]

Consent

The data controller should obtain free, unambiguous, and informed consent from the individual before it can process the individual's personal data.[96] As explained above, it may be necessary to obtain consent from a third party if the individual is unable to provide adequate consent. Also, explicit consent may be needed to process sensitive information.

Data Controller's Legitimate Interest

The data controller's legitimate interests may justify the processing of an individual's personal data.[97] However, the legitimate interests and rights of the individual must be balanced against the interests of the data controller.[98] If the interests of the individual prevail, then the individual's data should not be processed.[99]

Contractual Obligations

The processing of an individual's personal data may be allowed, if necessary, prior to or during the performance of a contractual relationship between the data controller and the individual.[100]

Legal Authority

The processing of the individual's personal data is permissible if it is necessary for the data controller to comply with a duty imposed by a government authority or it is carried out by a data controller, who is a public entity, in the legitimate exercise of its authority.[101] This condition also applies to law enforcement bodies that process personal data in the course of their investigative duties as authorized by the national legislature.[102]

Exceptional Circumstances

The processing of the individual's personal data is permissible if it is necessary to prevent or lessen an imminent and serious harm to the life, health, or the security of the individual or another person.[103] The data controller should reasonably believe that the processing of the individual's personal data is needed to prevent the harm.[104] The use of this condition as a basis to process personal data should not be used on a routine basis.[105] Furthermore, threats to financial security or reputation are not generally considered imminent and serious threats.[106]

Principle 7: Disclosures to Data Processors

The data controller may use data processors to process personal data. It will not be considered a disclosure to a third party, which would require notice to the individual whose data is being processed, if one of the following conditions exists.

Data Controller Ensures Level of Protection

It will not be a third party disclosure if the data controller makes sure that the data processor provides, at a minimum, the same level of protection as required by national legislation and the personal data protections set out in this document.[107]

Level of Protection Established through Contractual Relationship

It will not be a third party disclosure if the data controller and the data processor enter into a contractual relationship, which sets out the data processor's duty to comply with the data controller's instructions, which should guarantee the adequate protection of personal data.[108] The contract must also set out the appropriate security measures to ensure the protection of the personal data.[109] Further, once the contractual relationship ends, the data processor must properly destroy the personal data or return it to the data controller.[110]

Principle 8: International Transfers

International transfers of personal data should only be carried out if the receiving country, which is the destination country, offers, at a minimum, the same level of personal data protection, afforded by these principles.[111] Moreover, transit countries, which are countries where information is routed through and not processed, do not have to be in compliance.[112] However, the transfer of the personal data should still be secure.

To determine whether minimum data protection standards are afforded by a receiving country, the following factors should be analyzed: 1) the nature of the data; 2) the country of origin; 3) the receiving country; 4) the purpose for which the data is being processed; and 5) the security measures in place for the transfer and processing of the personal data.[113] In the event that the receiving country does not afford the same level of protection, the transfer of personal data may still occur if one of the following conditions exists and the processing is fair and lawful.[114]

Contractual Relationship Guarantees Level of Protection

Personal data may be transferred to a receiving country that does not afford, at a minimum, the same level of personal data protection as provided by these principles, if there is a contractual clause that makes compliance with the minimum level of data protection mandatory.[115]

National Legislation Permits the International Transfer

National legislation may allow the transferring of personal data to a third country that does not afford the same level of protection if one of the following conditions applies: 1) the transfer is necessary and in the interest of the individual in a contractual relationship; 2) the transfer is necessary to protect a vital interest, such as preventing substantial harm or death, of the individual or another person; or 3) the transfer is legally allowed to protect a public interest.[116]

Consent

The transfer of personal data to a receiving country that does not afford the minimum level of protection may be allowed if the individual unambiguously consents to the transfer.[117]

Principle 9: Individual's Right of Access

The right of access is the individual's right to request and obtain information about the individual's personal data from the data controller.[118] The individual may not have the right of access to personal data if the disclosure would likely have an unreasonable impact on a third party's privacy and rights unless the third party's information is severed or the third party consents to the disclosure.[119] It should be noted that the right of access provides the individual with the right to see the individual's personal data information, instead of the documents containing the information.[120]

Personal Data That May Be Requested and Disclosed

An individual may request information about a specific data subject and/or how and why the personal data is being processed.[121] The latter includes information regarding the source of the personal data, the purpose of processing, and to whom, which may include categories of recipients, the personal data will be disclosed.[122] Unless personal data is routinely amended and/or deleted, the personal data held by data controller at the time that the request was made should be disclosed.[123] However, if personal data is routinely amended and/or deleted, then the personal data held at the time that the data controller responds to the request may be disclosed instead.[124]

How and When Should Personal Data be Disclosed

As required by the transparency principle noted above, all information provided to the individual should be clear and easily understood.[125] The data controller may provide a copy of the personal data or display the personal data for the individual's inspection. Additionally, the data controller may provide personal data information to an individual at a charge that is not excessive or free.[126] Further, national legislation may require the data controller to respond to personal data requests within a reasonable amount of time depending on the amount and type of personal data information requested.[127]

Repetitive Requests

National legislation may limit how many times during a limited time period a data controller must respond to personal data requests made by the individual.[128] The purpose of this rule is to limit repetitive requests made by an individual during a short period of time.[129] However, if the individual presents a legitimate reason for repeatedly requesting access to personal data, then the data controller may still be required to respond.[130]

Principle 10: Individual's Right to Correct and Delete Personal Data

The individual has the right to request that the data controller correct or delete personal data that may be "incomplete, inaccurate, unnecessary, or excessive."[131] While the data controller is in the correction or deletion process, the data controller may either block access or indicate that the personal data is under revision before disclosing its contents to third parties.[132]

Reasonable Corrections and Deletions

If the correction or deletion is reasonable, then the data controller should correct or delete the personal data as requested by the individual.[133] If the personal data has been disclosed to third parties, then the data controller should also notify third parties, if known, of the change.[134]

Unreasonable Corrections and Deletions

If the individual requests correction or deletion of personal data and the personal data must be retained for the performance of a duty imposed on the data controller by national legislation or because of a contractual relationship between the data controller and the individual, then the correction or deletion of the personal data is not reasonable.[135]

Principle 11: Right to Object to the Processing of Personal Data

The individual may object to the processing of the individual's personal data where there is a legitimate reason, such as an "unwarranted and substantial damage or distress" to the individual.[136] The individual should specify why the processing of personal data has this effect.[137] The individual may only object to the processing of the individual's own personal data.[138] The individual may not object to the processing of the individual's personal data if it is necessary for the performance of a duty imposed on the data controller by national legislation, necessary for the performance of a contractual duty between the data controller and the individual, or the individual has consented.[139]

Principle 12: Standing to Exercise Personal Data Processing Rights

Individuals and third party representatives may exercise the right of access, the right to correct and delete, and the right to object over personal data processing.[140]

The Individual

The individual may exercise direct control over the individual's own personal data.[141] The data controller may require the individual to provide reasonable information to determine the individual's identity.[142]

Third Party Representatives

National legislation may allow heirs to have standing to exercise rights over an individual's personal data in the event of the individual's death.[143] In addition, lawyers and other persons acting on behalf of the individual may have standing to exercise rights over the individual's personal data.[144] However, the data controller must be adequately satisfied that the third parties have the appropriate authority to act on behalf of the individual.[145]

Procedures for the Exercise of Rights

The data controller must have procedures in place that allow individuals to exercise the right of access, right of correction and deletion, and the right to object easily, quickly, and efficiently.[146] Further, the procedures should not involve unnecessary delays, costs, or provide any advantage to the data controller.[147]

National Legislation Limiting or Denying the Exercise of Rights

National legislation may limit or deny the ability of the individual or third party representatives to exercise the right of access, right of correction and deletion, and the right to object.[148] However, the data controller should inform the individual or third party representatives the reasons behind the decision limiting or denying the exercise of those rights unless it would prejudice an investigation against unlawful activity.[149]

Principle 13: Security Measures to Protect Personal Data

The data controller and the data processor must provide reasonable "technical and organization measures" to guarantee the personal data's integrity, confidentially, and availability.[150] The measures that the data controller and the data processor must provide will depend on how personal data is processed, the consequences to the individual if there is a breach, its sensitive nature, and any duties imposed by national legislation.[151] In addition, the data controller must take reasonable steps to destroy, dispose, or permanently remove identification information from personal data that is no longer needed for processing.[152]

Security Breaches

The data controller should inform the individual of any security breaches that could significantly affect the individual's rights and any steps taken to resolve the breach.[153] The information should be provided in a reasonable amount of time so the individual may be able to take steps to protect the individual's rights.[154]

Principle 14: Duty of Confidentiality

The data controllers and data processors have the duty to keep all personal data confidential.[155] The duty of confidentiality extends after the relationship ends between the individual and the data controller, or the data processor and the data controller.[156] However, the duty of confidentiality may be discharged by a court if necessary to protect public safety, national security, or public health.[157]

Principle 15: Monitoring, Compliance, and Liability

To ensure compliance and enforce data protection principles, OAS member states should have a supervisory authority and provide judicial recourse to the individual. Moreover, data controllers and data processors who fail to process personal data as provided by the applicable national legislation may be subject to administrative, civil, or criminal liabilities.

Supervisory Authority

OAS member states should have an authority that is responsible for supervising the compliance of these data protection principles and the applicable national legislation.[158] The supervising authority should be impartial and independent.[159] It should have the technical capability, sufficient power, and adequate resources to conduct investigations and audits to ensure compliance.[160] It should also be able to impose financial penalties for noncompliance.[161] The supervisory authority should also be able to handle claims alleging data protection violations and provide administrative remedies to the individual.[162]

Moreover, an organization that may be planning to process personal data may be required to report its intention to do so to the supervisory authority before processing is allowed to begin.[163] Data controllers may also be required to report to the supervisory authority any changes in the use and purpose of its personal data processing.[164]

National legislation may provide the supervisory authority with the power to allow or deny some or all international transfers of personal data within its jurisdiction.[165] Data controllers planning on transferring personal data to third countries should be able to show to the supervisory authority that the transfer of personal data complies with these principles and the applicable national legislation.[166]

Judicial Recourse

Without prejudice to any administrative remedy provided by a supervisory authority, individuals should also have recourse in the national court system to enforce data protection rights afforded by national legislation.[167] Under applicable legislation, an individual may be entitled to damages if the individual suffered harm as a result of the data controller's failure to protect the individual's personal data.[168] Further, the courts may also provide judicial review of administrative decisions made by a supervisory authority.[169] In addition, some serious violations of personal data protections afforded by national legislation may be prosecuted as criminal offenses.[170]

VI. PROACTIVE MEASURES AND COOPERATION

OAS member states, aware of the discrepancy between regulation and technology, should consider proactive measures and cooperate to promote the protection of personal data. These measures will become increasingly necessary as technology continues to evolve, and OAS member states become more technologically interconnected with each other and other countries from other regions of the world.

Proactive Measures

As a result, OAS member states should consider the creation and implementation of training, education, and public awareness programs for the public and government officials to promote the understanding of personal data protection legislation, procedures, and rights.[171] OAS members states should also create standard operating procedures for data controllers to follow to prevent, detect, and contain a security breach if it happens.[172] OAS member states should encourage audits by an independent party or civil society to assess and verify compliance with data protection laws.[173] In addition, OAS

member states should encourage the creation of working groups, seminars, and workshops designed to promote and share best practices in personal data protection.[174]

Cooperation

National authorities involved in the protection of personal data should also be encouraged to cooperate and coordinate with each other at the national and international levels to promote the uniform and adequate protection of personal data.[175] In the event of an investigation, national authorities should be encouraged to cooperate and coordinate with each other and international agencies.[176] As with all of the above principles, cooperation between national and international authorities is an essential part of personal data protection.

Conclusions of the Inter-American Juridical Committee

The Inter-American Juridical Committee, in its 2007 report on the issue provided the following conclusions: "The protection of personal information and data held in electronic form in the private sector has been advanced through the establishment of international instruments. The OECD Guidelines, the European Council Convention, the UN Guidelines, and particularly the EU Data Protection Directive have had a profound impact on data protection in Europe and elsewhere. Also some OAS countries, notably Canada and Chile, have enacted laws which provide relatively high levels of privacy protection. Nevertheless, it seems fair to say that many challenges remain particularly with respect to the transborder flow of personal data on the Internet and other global networks. The privacy of citizens remains vulnerable even in those countries which have effective national laws, because of the existence of data havens where no protection is available. The existing international and national instruments leave numerous problems unresolved, such as the interpretation of what "adequate" and "equivalent" levels of protection are or the nature of the enforcement required to implement agreed upon standards. Legislation and enforcement are especially challenging because of rapidly evolving technology. In addition, those States who wish to protect the privacy of their citizens are also faced with competing economic, trade, social and political interests.

These difficulties, however, are not unique to the area of data protection. Further progress in the area of privacy protection could probably be made by a combination of measures, including the development of international standards and enforcement mechanisms, mutual legal and technical assistance, the encouragement of industry self-regulation, and the operation of market forces influenced by information and education."

Conclusion

Finally, OAS member states should continue studying the topic and consider updating their regulatory systems to protect personal data based on the principles and recommendations contained herein, focused primarily to safeguard an individual's right to privacy. They should apply in all circumstances of government and/or private party collection, custody, control and transfer of the data. They should also apply to all circumstances where a third party may have the right to access that information under access to information legislation.

These preliminary principles and recommendations have served as the basis for data protection legislation worldwide and can serve as the basis for new international instrument or domestic legislation on data protection in the Americas.

[1] Jean Sleemons Stratford and Juri Stratford, *Data Protection and Privacy in the United States and Europe*, IASSIST QUARTERLY, Fall 1998, at 19.
[2] Id. at 17.
[3] Id.
[4] Id. at 19.
[5] *See* Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data arts. 2, 4-12, Jan. 28, 1981.
[6] *See* Stratford, supra, at 19 (adding that the *Directive*, which was adopted in 1995, directed member states to ensure that their national privacy laws were in compliance with its standards).
[7] Id.
[8] Id. at 19-20.
[9] Id. at 17.
[10] Id. (quoting Samuel Warren and Louis Brandeis, who argued that the right to privacy given to "intellectual and artistic property" in American common law was "founded on that of the "inviolate personality").
[11] Id.
[12] Id.
[13] Id.
[14] Id. at 17-19 (noting that the *Privacy Act* and the *Computer Matching and Privacy Protection Act of 1988* are the two most important pieces of legislation in the United States protecting the right to privacy and data protection).
[15] *See also* id. at 19.
[16] Id. at 19-20.
[17] *See* Stratford, supra at 20.
[18] Andreas Guadamuz, *Habeas Data: An update on the Latin American data protection constitutional right*, BILETA, Jan. 4, 2005, http://www.bileta.ac.uk/01papers/guadamuz.html.
[19] *See* id.; Pablo Palazzi, *El Habeas Data en el Derecho Argentino*, REVISTA DE DERECHO INFORMÁTICO, Nov. 1998, http://www.alfa-redi.org/rdi-articulo.shtml.
[20] *See* Gaudamuz, supra.
[21] Id. (noting that sensitive personal data includes religion, political ideologies, and sexual orientation); Palazzi, supra (stating that Argentinean *Habeas Data* requires evidence of inaccurate information or discrimination in order to correct, rectify, or suppress the personal data).
[22] Id.
[23] Id. (noting that *Habeas Data* in Argentina does not allow an aggrieved person access to the personal data of a third party although there may be a link between the personal data of both individuals).
[24] Id.
[25] *See also* Personal Data Protection Act of Argentina No. 25.326, § 14, supra.
[26] Council of Europe, supra, at art. 2; *See* Organization of Economic Co-Operations and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data art. 1, Sept. 23, 1980 (noting that the Expert Group's Detailed Comments state that the Guidelines were concerned with the personal data of "physical persons").
[27] Spanish Data Protection Agency, International Standards on the Protection of Personal Data and Privacy: The Madrid Resolution, Nov. 5, 2009.
[28] Personal Data Protection Act of Argentina No. 25.326, § 1 (October 30, 2000).
[29] *See* Information Commissioner's Office, The Guide to Data Protection at 22 (adding that opinions or other expressions of intention regarding the individual is also personal data); Spanish Protection Agency, supra (defining "personal data" as "any information relating to an identified natural person").
[30] Organization of Economic Co-Operations and Development, supra, at art. 1.
[31] Council of Europe, supra, at art. 2.
[32] *See* Office of the Federal Privacy Commissioner, Guidelines to the National Privacy Principles, 23 (Sept. 2001) (observing that this legislation applies to private organizations); Personal Information Protection and Electronic Documents Act, Apr. 13, 2000, art. 2 (Can.) (noting that this legislation applies to private organizations); Information Commissioner's Office, supra, at 23; Organic Law 15/1999 of 13 December on the Protection of Personal Data, art. 7 (Dec. 13, 1999)(Spain). *See also* Privacy Act, June 1, 2009, art. 3 (Can.); Privacy Commissioner, Plain English Guidelines to Information Privacy 1 (1994) (observing that Canada's Privacy Act and Australia's Information Privacy Principles apply to the government).

[33] *See* Information Commissioner's Office, supra, at 27; Organic Law, supra, art. 3.
[34] Id.
[35] *See* Information Commissioner's Office, supra, at 28.
[36] Id. at 29.
[37] Id. at 23; Organic Law, supra, at art. 7.
[38] *See* Council of Europe, supra, at art. 2.
[39] *See* Information Commissioner's Office, supra, at 25.
[40] *See* Spanish Protection Agency, supra.
[41] Id.
[42] *See* Information Commissioner's Office, supra, at 25.
[43] Id.
[44] *See* Spanish Protection Agency, supra.
[45] *See* Organic Law, supra, at art. 2.
[46] *See* Information Commissioner's Office, supra, at 115.
[47] Id.
[48] Id.
[49] *See* Spanish Protection Agency, supra.
[50] *See* Information Commissioner's Office, supra, at 115.
[51] *See* Privacy Commissioner, Plain English Guidelines to Information Privacy: Principles 8-11, supra, at 29.
[52] *See* Information Commissioner's Office, supra, at 116.
[53] Id.
[54] Id. at 51; Privacy Commissioner, supra, at 11.
[55] *See* Information Commissioner's Office, supra, at 51.
[56] *See* Spanish Protection Agency, supra.
[57] *See* Information Commissioner's Office, supra, at 43.
[58] Id. at 43, 45 (noting that sometimes the processing of personal data may have an adverse on an individual, but will not be deemed unfair if, for example, it is related to legitimate purpose, such as law enforcement).
[59] *See* Information Commissioner's Office, supra, at 43, 46.
[60] Id. at 43, 47 (adding that privacy notices should include the identity of who is collecting the personal data, its intended use, and any other information that would need to be disclosed to the individual so the personal data can be processed fairly).
[61] Id. at 47.
[62] *See* Spanish Protection Agency, supra.
[63] *See* Information Commissioner's Office, supra, at 54.
[64] Id. at 53. *See also* Office of the Federal Privacy Commissioner, supra, at 36 (stating that the test for "reasonable expectation" should be "what an individual with no special knowledge of the industry or activity involved would expect").
[65] *See* Office of the Federal Privacy Commissioner, supra, at 33.
[66] *See* Spanish Protection Agency, supra.
[67] *See* Information Commissioner's Office, supra, at 54, 56.
[68] *See* Office of the Federal Privacy Commissioner, supra, at 35.
[69] Id.
[70] *See* Spanish Protection Agency, supra.
[71] *See* Privacy Commissioner, Plain English Guidelines to Information Privacy: Principles 1-3, supra, at 6.
[72] *See* Information Commissioner's Office, supra, at 59 (noting that if certain personal information is needed for certain individuals only, then the collection and processing of that information for other individuals will be deemed excessive).
[73] Id.
[74] *See* Organization of Economic Co-Operations and Development, supra, at art. 10.
[75] *See* Spanish Protection Agency, supra.
[76] *See* Office of the Federal Privacy Commissioner, supra, at 27 (adding that collecting personal data on the remote chance that it is may become necessary in the future is not acceptable).
[77] *See* Privacy Commissioner, Plain English Guidelines to Information Privacy: Principles 1-3, supra, at 6.
[78] *See* Information Commissioner's Office, supra, at 114.
[79] *See* Data Protection Act of 1998 of the United Kingdom, § 1 (1998).

[80] *See* Information Commissioner's Office, supra, at 61.
[81] Id. at 7.
[82] *See* Spanish Protection Agency, supra.
[83] *See* Privacy Commissioner, Plain English Guidelines to Information Privacy: Principles 1-3, supra, at 17.
[84] *See also* Information Commissioner's Office, supra, at 8.
[85] *See* Spanish Protection Agency, supra.
[86] Id.
[87] Id.
[88] Id.
[89] *See* Personal Data Protection Act of Argentina No. 25.326, supra, § 15.
[90] *See* Information Commissioner's Office, supra, at 125.
[91] *See* Spanish Protection Agency, supra; Information Commissioner's Office, supra, at 125.
[92] *See* Spanish Protection Agency, supra.
[93] Id.
[94] *See* Federal Privacy Commissioner, supra, at 47-48.
[95] *See* Spanish Protection Agency, supra; Information Commissioner's Office, supra, at 112.
[96] *See* Spanish Protection Agency, supra.
[97] Id.
[98] *See* Information Commissioner's Office, supra, at 111.
[99] *See* Spanish Protection Agency, supra.
[100] Id.
[101] Id.
[102] *See* Office of the Federal Privacy Commissioner, supra, at 41.
[103] *See* Spanish Protection Agency, supra; Privacy Commissioner, Plain English Guidelines to Information Privacy: Principles 8-11, supra, at 38.
[104] *See* Privacy Commissioner, Plain English Guidelines to Information Privacy: Principles 8-11, supra, at 37.
[105] Id. at 22.
[106] *See* Office of the Federal Privacy Commissioner, supra, at 40.
[107] *See* Spanish Protection Agency, supra.
[108] Id.; *See* Organic Law, supra, at art. 12 (observing that the data processor is responsible for any personal data disclosures not made in accordance with the contract).
[109] *See* Organic Law, supra, at art. 12.
[110] Id.
[111] *See* Spanish Protection Agency, supra.
[112] *See* Information Commissioner's Office, supra, at 95.
[113] *See* Data Protection Act of 1998 of the United Kingdom, § 8, supra.
[114] *See* Information Commissioner's Office, supra, at 94.
[115] *See* Spanish Protection Agency, supra.
[116] *See also* id.
[117] *See* Office of the Privacy Commissioner, supra, at 58.
[118] *See also* Spanish Protection Agency, supra.
[119] *See* Personal Information Protection and Electronic Documents Act, supra, at art. 8; Office of the Federal Privacy Commissioner, supra, at 50; Information Commissioner's Office, supra, at 133.
[120] *See* Information Commissioner's Office, supra, at 123.
[121] *See* Spanish Protection Agency, supra.
[122] Id.
[123] *See* Information Commissioner's Office, supra, at 125.
[124] Id. (stating that amendments to personal data made to prevent disclosure are not allowed).
[125] *See* Spanish Protection Agency, supra.
[126] *See* Organization of Economic Co-Operations and Development, supra, at art. 13; Organic Law, supra, at art. 15; Office of the Federal Privacy Commissioner, supra, at 127 (observing that a data controller cannot ignore a request for access to personal data because the individual has not paid the requisite fee).
[127] *See also* Personal Data Protection Act of Argentina No. 25.326, § 14, supra; Office of the Federal Privacy Commissioner, supra, at 49.
[128] *See* Spanish Protection Agency, supra.

[129] Id.
[130] Id.
[131] Id.
[132] *See* Organic Law, supra, at art. 16.
[133] *See* Spanish Protection Agency, supra.
[134] *See also* id.
[135] Id.
[136] Id.; Information Commissioner's Office, supra, at 137.
[137] *See* Information Commissioner's Office, supra, at 137.
[138] Id.
[139] Id. at 137-38; Spanish Protection Agency, supra.
[140] *See* Spanish Protection Agency, supra.
[141] Id.
[142] *See* Personal Data Protection Act of Argentina No. 25.326, § 14, supra; Information Commissioner's Office, supra, at 127.
[143] *See* Personal Data Protection Act of Argentina No. 25.326, § 14, supra.
[144] Id.
[145] *See* Information Commissioner's Office, supra, at 129-30.
[146] *See* Spanish Protection Agency, supra.
[147] Id.
[148] Id.
[149] *See* Spanish Protection Agency, supra; Office of the Federal Privacy Commissioner, supra, at 54. *See also* Organization of Economic Co-Operations and Development, supra, at art. 11.
[150] *See* Spanish Protection Agency, supra.
[151] Id.; Office of the Federal Privacy Commissioner, supra, at 44-45.
[152] Office of the Federal Privacy Commissioner, supra, at 45-46.
[153] *See* Spanish Protection Agency, supra.
[154] Id.
[155] Id.
[156] Id.
[157] *See* Personal Data Protection Act of Argentina No. 25.326, § 10, supra.
[158] *See* Spanish Protection Agency, supra.
[159] Id.
[160] *See* Spanish Protection Agency, supra; Information Commissioner's Office, supra, at 14.
[161] Id.
[162] *See* Spanish Protection Agency, supra.
[163] *See* Organic Law, supra, at art. 26.
[164] Id.
[165] *See* Spanish Protection Agency, supra.
[166] Id.
[167] *See* Spanish Protection Agency, supra.
[168] *See* Organic Law, supra, at art. 19.
[169] *See* Spanish Protection Agency, supra.
[170] *See* Personal Data Protection Act of Argentina No. 25.326, § 32, supra; Information Commissioner's Office, supra, at 16-17.
[171] *See also* Spanish Protection Agency, supra.
[172] Id.
[173] *See* id.
[174] Id.
[175] Id.
[176] Id.