97th REGULAR SESSION
3 –7 August 2020
Virtual Session

OEA/Ser. Q
CJI/doc. 616/20 rev.1 corr.1
7 August, 2020
Original: Spanish/English

INTERAMERICAN JURIDICAL COMMITTEE (CJI)

DRAFT UPDATES TO THE "*PRINCIPLES ON PRIVACY AND PERSONAL DATA PROTECTION, WITH ANNOTATIONS*" ADOPTED BY THE IAJC IN 2015

FOR COMMENTS BY OAS MEMBER STATES

For ease of reference, some of the proposed updates are followed by temporary bracketed text indicating the cross-reference to similar provisions contained in other international instruments regarding data protection, namely:

- *The Personal Data Protection Standards for Ibero-American States, adopted by the Ibero-American Network for Data Protection on June 20, 2017 (hereinafter, the "Ibero-American Standards");*
- *The General Data Protection Regulation of the European Union, in force since May 25, 2018 (hereinafter "GDPR");*
- *The California Consumer Privacy Act, in force since January 1, 2020 (hereinafter "CCPA").*
- *The Decision of the Secretary-General of the Organization for Economic Cooperation and Development (OECD) on the Protection of Individuals with regard to the Processing of their Personal Data, effective as from 3 May 2019 (the "OECD Decision").*
- *Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) Framework, which implements the APEC Privacy Framework updated in 2015 (hereinafter "APEC CBPR").*
- *United States Mexico Canada Agreement, in force since July 1, 2020 (hereinafter "USMCA").*

UPDATED OAS PRINCIPLES ON PRIVACY AND PERSONAL DATA PROTECTION, WITH ANNOTATIONS

I. THE PRINCIPLES

FIRST PRINCIPLE
Lawful and Fair Purposes

Personal data should be collected only for lawful purposes and by fair and lawful means.

SECOND PRINCIPLE
Transparency and Consent

The categories of personal data to be collected, the purposes for which personal data is collected and shall be used, the recipients or categories of recipients to whom the personal data have been or will be disclosed, and the rights that the data subject will have regarding personal data to be collected, should be specified at or before the time the data is collected. When processing is based on consent, personal data should only be collected with the consent of the individual concerned.

THIRD PRINCIPLE
Relevance and Necessity

The data should be relevant and necessary to the stated purposes for which it is collected.

FOURTH PRINCIPLE
Limited Use and Retention

Personal data should be kept and used only in a lawful manner not incompatible with the purpose(s) for which it was collected. It should not be kept for longer than necessary for that purpose or purposes and in accordance with relevant domestic law.

FIFTH PRINCIPLE
Duty of Confidentiality

Personal data should not be disclosed, made available or used for purposes other than those for which it was collected except with the knowledge or consent of the concerned individual or under the authority of law.

SIXTH PRINCIPLE
Protection and Security

The confidentiality, integrity and availability of personal data should be protected by reasonable and appropriate technical or organizational security safeguards against unauthorized or unlawful processing and against accidental loss, destruction or damage.

SEVENTH PRINCIPLE
Accuracy of Data

Personal data should be kept correct, accurate, complete and up-to-date to the extent necessary for the purposes for which it was collected.

EIGHTH PRINCIPLE
Access, Rectification, Erasure, Objection and Portability

Reasonable methods should be available to permit individuals whose personal data has been collected the rights to access, obtain rectification, and obtain erasure of personal data regarding them, as well as the right to object to its processing and, where applicable, the right to data portability thereof. As a general rule, the exercise of such rights should be free of cost. Should it be necessary to curtail the scope of these rights, the specific grounds for any such restrictions should be specified in accordance with domestic law.

NINTH PRINCIPLE
Sensitive Personal Data

Some types of personal data, given its sensitivity in particular contexts, are especially likely to cause material harm to individuals if misused. Data controllers should adopt privacy and security measures that are commensurate with the sensitivity of the data and its capacity to harm individual data subjects.

TENTH PRINCIPLE
Accountability

Data controllers should adopt and implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with these Principles.

The data controller and processor and, where applicable, their representatives, should cooperate, on request, with the data processing authority in the performance of their tasks.

ELEVENTH PRINCIPLE
Trans-Border Flow of Data and Accountability

Member States should cooperate with one another in developing mechanisms and procedures to ensure that data controllers and processors operating in more than one jurisdiction can be effectively held accountable for their adherence to these Principles.

TWELFTH PRINCIPLE
Exceptions

When national authorities make exceptions to these Principles for reasons relating to national sovereignty, national security, public security, protection of public health, the fight against criminality, regulatory compliance or other public order policies, the protection of rights and freedoms of others, or public interest, they should establish them specifically by a law or norm and make those exceptions known to the public.

THIRTEENTH PRINCIPLE
Data Protection Authorities

Member States should establish independent supervisory bodies, in accordance with each State's constitutional, organizational and administrative structure, to monitor and promote the protection of personal data in consistency with these Principles.

II. THE ANNOTATIONS

Introduction

The purpose of updating the "Principles on Privacy and Personal Data Protection" adopted by the Inter American Juridical Committee (CJI) in 2015 is to contribute to the development of a current framework for safeguarding the rights of the individual to personal data protection and informational self-determination in the countries of the Americas. The Principles are based on internationally recognized norms and standards, as these have evolved up until 2020. They are intended to support Member States' efforts to protect individuals from wrongful or unnecessary collection, use, retention and disclosure of personal data.

The following elaboration of the Principles is intended to provide a guide to the preparation, updating and implementation of national legislation and related rules within OAS Member States.

Each Member State should decide how best to implement these Principles in its domestic legal system. Whether by means of legislation, regulations or other mechanisms, Member States should establish effective rules for personal data protection that give effect to the individual's right to privacy and demonstrate respect for their personal data, while at the same time safeguarding that the individual may benefit from the free flow of information and access to the digital economy.

These Principles aim to provide the basic elements of effective protection. States may provide additional mechanisms to ensure the privacy and protection of personal data while taking into account the legitimate functions and purposes for which personal data is collected and used for the benefit of

individuals. Overall, the Principles reflect the importance of effectiveness, reasonableness, proportionality and flexibility as guiding elements.

Scope

These Principles apply equally to the public and private sectors – that is, to personal data generated, collected or administered by government entities as well as to data gathered and processed by private entities.[1] They apply to personal data contained in hard copy as well as electronic files. They do not apply to personal data used by an individual exclusively in the context of his or her private, family or domestic life. Neither do they apply to anonymous information, meaning data unrelated to an identified or identifiable natural person, as well as personal data that has gone through an anonymization process in such a way that the subject cannot be identified or reidentified *(cf.* definition of 'anonymization', *infra*).

[NOTE: Based on N° 4.3 of the Ibero-American Standards]

The Principles are interrelated and should be interpreted together as a whole.

The Concept of Privacy

The concept of privacy is well-established in international law. It rests on fundamental concepts of personal honor and dignity as well as freedom of speech, thought, opinion and association. Provisions on the protection of privacy, personal honor and dignity are found in all the major human rights systems of the world.

Within our own hemisphere, these concepts are clearly established in Article V of the American Declaration of the Rights and Duties of Man (1948) as well as Articles 11 and 13 of the American Convention on Human Rights ("Pact of San Jose") (1969). (Appendix A.) The right to privacy has been upheld by the Inter-American Court of Human Rights.[2]

In addition, the constitutions and fundamental laws of many OAS Member States guarantee respect and protection for personal data as distinct and complementary to the rights of privacy, personal dignity and family honor, the inviolability of home and private communications and related concepts. Almost all OAS Member States have adopted some form of legislation regarding privacy and data protection (although their provisions vary in approach, scope and content). Consistent with these fundamental rights, the OAS Principles reflect the concepts of informational self-determination, freedom from arbitrary restrictions on access to personal data, and protection of privacy, identity, dignity and reputation.

[Note: Based on preambular paragraph (2) of the Ibero-American Standards]

At the same time, as recognized in all legal systems, the right to privacy is not absolute and can be restricted by reasonable limitations rationally related to appropriate goals.

---

[1] Regarding the specific right of individuals to access public information, see the Model Inter-American Law on Access to Public Information, adopted by the OAS General Assembly on June 8, 2010 in AG/RES. 2607 (XL-O/10), which incorporates the principles outlined by the Inter-American Court on Human Rights in *Claude Reyes v. Chile*, Judgment of Sept. 19, 2006 (Series C No. 151), as well as the Principles on Access to Information adopted by the Inter-American Juridical Committee in CJI/RES. 147 (LXXIII-O/08).

[2] "[T]he sphere of privacy is characterized by being exempt and immune from abusive and arbitrary invasion by third parties or public authorities." Case of the Ituango Massacres v. Colombia, Judgment of July 1, 2006 (para. 149), available at http://www.corteidh.or.cr/docs/casos/articulos/seriec_148_ing.pdf.

The Concept of Free Flow of Information

Similarly, the fundamental principles of freedom of expression and association, and the free flow of information, are recognized in all the major human rights systems of the world, including within the Inter-American System, for example in Article IV of the American Declaration of the Rights and Duties of Man (1948) as well as Article 13 of the American Convention. (Appendix A). These essential civil and political rights are reflected throughout our hemisphere in the constitutions and fundamental laws of every OAS Member States (although, again, their provisions vary in approach, scope and content). They are central to the promotion of democracy and democratic institutions.

In a people-centered and development-oriented "information society," protecting the right of individuals to access, use and share information and knowledge can enable individuals, communities and peoples to achieve their full potential, to promote sustainable development, and to improve the overall quality of life, consistent with the purposes and principles of the OAS Charter and our regional human rights instruments.

Definitions

Anonymization. As used in these Principles, the term "anonymization" refers to the adoption of measures of any nature aimed at preventing the identification or reidentification of a natural person without disproportionate effort.

[NOTE: Based on Nº 2.1(a) of the Ibero-American Standards]

Personal Data. As used in these Principles, the term "personal data" includes information that identifies, or can be reasonably be used to identify, a natural person, whether directly or indirectly, in particular by reference to an identification number, location data, an online identifier or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity. It includes information expressed in a numerical, alphabetical, graphic, photographic, alpha-numerical, audio, electronic, visual or any other manner. The term does not include information that does not identify (or cannot reasonably be used to identify) a particular individual.

[NOTE: Based on Article 4.1 of the GDPR, article 2.c of the Ibero-American Standards and §1798.140(o)(1) of CCPA]

The Principles intentionally use the term "data" broadly in an effort to provide the broadest protection to the rights of the individuals concerned, without regard to the particular form in which the data is collected, stored, retrieved, used or disseminated. The Principles generally avoid using "personal information" since that term might be construed by itself not to include specific "data" such as factual items or electronically-stored "bits" or digital records. Similarly, the term "data" might be construed not to include compilations of facts that taken together allow conclusions to be drawn about the particular individual(s). To illustrate, details about the height, weight, hair color and date of birth of two individuals might be "data" which, when compared, might reveal the "information" that they are brother and sister or perhaps identical twins. To promote the greatest protection of privacy, these Principles would apply in both situations and would not permit a data controller to make such distinctions.

Examples of personal data include identifiers such as real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number or other similar identifiers, or commercial information, biometric information, internet or other electronic network activity information (such as browsing history, search history and information regarding a data subject's interaction with an internet website, application, or advertisement, geolocation data, audio, electronic, visual, thermal, olfactory or similar information, professional or employment-related information, educational information and

inferences drawn from the above to create a profile about the data subject's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes, among others.

[NOTE: Based on §1798.140(o))1) of the CCPA]

For purposes of these Principles, only people (natural persons) have privacy interests -- not the devices, computers or systems by which they interact. Neither do the organizations or other legal entities with which they deal. Minors (individuals below the age of adulthood) also have legitimate privacy interests which should be recognized and effectively protected by national law.

Data Controller. As used in these Principles, the term "data controller" refers to the natural or legal person, private entity, public authority or other body or organization or service (alone or jointly with others) with responsibility for the storage, processing, use, protection and dissemination of the personal data in question. In general, it will include the natural or legal persons or authorities empowered under national law to decide the content, purpose and use of a data file or data base. In some circumstances, the term will also apply to entities which can be described as "data collectors" since in most situations the entity that stores, uses, and disseminates the personal data will also be responsible (directly or indirectly) for collecting that data.

[NOTE: Based on Nº 2.1 (g) of the Ibero-American Standards and article 4.7 of the GDPR]

Data Processor. The term "data processor" refers more specifically to the natural or legal person, private entity, public authority or other body or organization that (alone or jointly with others) processes the data in question. In general and for the vast majority of the States in the Americas region, the data processor is separate from the data collector and acts on behalf of and in the name thereof. In some situations, the data controller might also be the data processor, or the data controller may make arrangements for others to do the processing through a contractual relationship. The term "data processing" is used broadly, to include any operation or set of operations performed on personal data, such as collection, recording, storage, alteration, retrieval, disclosure, or transfer.

[NOTE: Based on Nº 2.1 (e) of the Ibero-American Standards and article 4.8 of the GDPR]

Data Protection Authority. As used in these Principles, the term "data protection authority" refers to the supervisory authorities established in Member States, empowered with setting and enforcing the laws, regulations and requirements relating to the protection of personal data, either at the national, regional or municipal level and in accordance with each State's constitutional, organizational and administrative structure.

[NOTE: Based on article 4.8 of the GDPR]

Data Subject. This term refers to the individual whose personal data is being collected, processed, stored, used or disseminated.

Sensitive Personal Data. The term "sensitive personal data" refers to a narrower category that includes data affecting the most intimate aspects of natural persons. Depending on the specific cultural, social or political context, this category might, for example, include data related to an individual's personal health, sex life or sexual preferences, religious, philosophical or moral beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, political opinions or racial or ethnic origins. In certain circumstances, this data might be considered worthy of special protection because, if mishandled or improperly disclosed, it could lead to serious harm to the individual or to unlawful or arbitrary discrimination.

[NOTE: Based on Nº 2.1 (d) and 9 of the Ibero-American Standards and on article 9 of GDPR and article 4.2 of the OECD Decision]

The Principles recognize that the sensitivity of personal data can be culture-specific, that it can change over time, and that the risks of actual harm to a person resulting from disclosure of such data can be negligible in one particular situation and life-threatening in another.

PRINCIPLES ON PRIVACY AND PERSONAL DATA PROTECTION, WITH ANNOTATIONS

FIRST PRINCIPLE: LAWFUL AND FAIR PURPOSES

Personal data should be collected only for lawful purposes and by fair and lawful means.

This Principle addresses two elements: (i) the "lawful purposes" for which personal data is initially collected and (ii) the "fair and lawful means" by which that data is initially collected.

The premise is that many if not most intrusions on the rights of individuals can be avoided if respect is given to the related concepts of lawfulness and fairness at the outset, when data is initially collected. These Principles of course apply and should be respected throughout the process of gathering, compiling, storing, using, disclosing and disposing of personal data -- not just at the point of collection. Yet they are more likely to be honored and respected if they are emphasized and respected from the very beginning.

Lawful Purposes

The requirement of lawfulness in the purpose for which personal data is collected, retained and processed is a fundamental norm, deeply rooted in basic democratic values and the rule of law. In principle, the collection of personal data should be limited and undertaken on the basis of the individual's knowledge or consent. Data should not be collected about individuals except in situations, and by methods, permitted or authorized by law and (as a general rule) disclosed to those concerned at the time of collection.

Member States should, therefore, include in their national legislations specific provisions on the lawful purposes of personal data processing. As a general rule, these should include cases when: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for the compliance with a legal obligation to which the data controller is subject; (d) processing is necessary to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party; (g) processing is necessary for compliance with a judicial order, resolution or mandate from a competent public authority; and (h) processing is necessary for the recognition or defense of the rights of the data subject before a competent public authority.

[NOTE: Based on article 6.1 of GDPR and Nº 11.1 of the Ibero-American Standards]

The requirement of lawfulness embraces the notion of legitimacy and excludes the arbitrary and capricious collection of personal data. It implies transparency and a legal structure that is accessible to the person whose data is being collected.

In most contexts, the lawfulness requirement can be respected if the data collector or processor informs the data subject about the legal basis on which the data is being requested at the time of collection

(e.g., "your personal identification number is requested pursuant to the National Registration Law of 2004" or "Ministry of Economy Directive 33-25," etc.).

In other situations, a different explanation may be required, such as "This information is required in order to guarantee that the refund of money is sent to the correct address of the claimant.…" In such cases, the purposes for which the data is collected should be stated clearly so that the individual is able to understand how the data will be collected, used or disclosed.

Fair and Lawful Means

This Principle also requires that the means by which the personal data is collected should be both "fair and lawful." Personal data is collected by fair and lawful means when the collection is consistent with both the applicable legal requirements and the reasonable expectations of individuals based on their relationship with the data controller or other entity collecting the data and the notice(s) provided to individuals at the time their data is collected.

This Principle excludes obtaining personal data by means of fraud, deception or under false pretenses. It would be violated, for example, when an organization misrepresents itself as another entity in telemarketing calls, print advertising, or email in order to deceive subjects and induce them to disclose their credit card numbers, bank account data or other sensitive personal information.

[Based on No. 15 of the Ibero-American Standards]

"Fairness" is contextual and depends on the circumstances. It requires, among other things, that individuals should be provided appropriate choices about how and when they provide personal data to data controllers when collection would not be reasonably expected given their relationships with the data collector or processor and the notice(s) they were provided at the time their data was collected. The choices provided to individuals should not interfere with the efforts and obligations of data controllers to promote safety, security, and legal compliance, or otherwise prevent them from engaging in commonly accepted practices regarding the collection and use of personal data.

In implementing these Principles, Member States may decide to contain a separate "fairness" requirement that is distinct from the issue of deception.

SECOND PRINCIPLE: TRANSPARENCY-AND CONSENT

The categories of personal data to be collected, the purposes for which personal data is collected and shall be used, the recipients or categories of recipient to whom the personal data have been or will be disclosed, and the rights that the data subject will have regarding personal data to be collected, should be specified at or before the time the data is collected. When processing is based on consent, personal data should only be collected with the consent of the individual concerned.

[NOTE: Based on Nº 12,16 and 25 of the Ibero-American Standards; article15 of GDPR and §1798.100(b) and §1798.110(a)(4) and (b)(4) of CCPA]

This Principle also focuses on the collection of personal data. It rests on the concept of "informational self-determination" and in particular on two basic concepts which are widely recognized internationally: the "transparency" principle and the "consent" principle. Together, they require that (i) the categories of personal data to be collected, the purposes for which personal data is collected and shall be used, as well as the recipients or categories of recipient to whom the personal data will be disclosed, and the rights that the data subject will have regarding personal data to be collected should be specified

generally not later than the point at which collection begins, and (ii) when processing is based on consent, personal data should only be collected with the clear consent of the individual concerned.

Transparency

The categories of personal data to be collected, the purposes for which personal data is collected and shall be used, as well as the recipients or categories of recipient to whom the personal data will be disclosed, and the rights that the data subject will have regarding personal data to be collected should be specified clearly at or before the time the data is collected. In addition, individuals should be informed about the practices and policies of the entities or persons collecting the personal data so they are able to make an informed decision about providing that data. Without clarity, the individual's agreement to collection cannot be meaningful.

In order to permit individuals to make informed decisions as to whom and for what reason they will provide their personal data, more information is needed than just the categories, purposes of the collection and handling of those data. It is also important for the individuals to be informed about the legal basis for such collection, how their personal data will be stored and processed, the identity and contact information of the personnel responsible for handling them, any data transfers that may be involved, the existence, forms and mechanisms or procedures at their disposal for exercising their rights to request from the data controller access, rectification or erasure of their personal data or to object to its processing, as well as their right to data portability and, where the personal data are not collected from the data subject, any available information as to their source.

[NOTE: Based on Nº 16.2 of the Ibero-American Standards, article 15 of GDPR and §1798.105(b) and §1798.110 of CCPA]

The information should be provided to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to children.

[NOTE: Based on article 12.1 of GDPR and Nº 16.3 of the Ibero-American Standards]

Consent

As a rule, the individual should be able to consent freely to the collection of personal data in the manner and for the purposes intended. The individual's consent should therefore be based on sufficient information and be clear, that is, leaving no doubt or ambiguity about the individual's intent. For consent to be valid, the individual should have sufficient information about the specific details of the data to be collected, how it is to be collected, the purposes of the processing, and any disclosures that may be made. The individual should have the ability to exercise a real choice.

There should be no risk of deception, intimidation, coercion or significant negative consequences to the individual from refusal to consent.

The method of obtaining consent should be appropriate to the age and capacity of the individual concerned (if known) and to the particular circumstances of the case. When obtaining the consent of children, the data controller should obtain authorization from the guardian or person *in loco parentis*, as set forth in the representation rules laid down in the internal law of the States, or should, if applicable, request authorization directly from the minor, should the domestic law of each State establish a minimum age for granting this directly and with no representation whatsoever from a guardian or person *in loco parentis*.

[*NOTE: Based on article 8 of GDPR and Nº 13.1 of the Ibero-American Standards]*

Consent should reflect the preference and informed decision by the individual concerned. Clearly, consent obtained under duress or on the basis of misrepresentations or even incomplete or misleading information cannot satisfy the conditions for legitimate collection or processing.

[*NOTE: Based on Nº 12.1 of the Ibero-American Standards]*

Context

The consent requirement should be interpreted reasonably in the rapidly evolving technological environment in which personal data is collected and used today. The nature of consent may differ depending on the specific circumstances. These Principles recognize that in some situations, "knowledge" may be the appropriate standard where personal data processing and disclosure satisfy legitimate interests. Implicit consent may be appropriate when the personal data in question is less sensitive and when information about the purpose and method of collection is provided in a reasonable way so that the requirements of transparency are satisfied.

For example, an individual's consent to the collection of some personal data may reasonably be inferred from previous interactions with (and notices provided by) data controllers and when collection is consistent with the context of the transaction for which data was originally collected. It may also be inferred from commonly accepted practices regarding the collection and use of personal data or the legal obligations of data controllers.

In some limited situations, non-consensual collection of some personal data may be authorized. In such instances, the party seeking to collect and process the data should show that it has a clear need to do so for the purposes of its legitimate interests or for those of a third party to whom the data may be disclosed. It should also demonstrate that the legitimate interests of the party seeking disclosure are balanced against the interests of the data subject concerned.

The "legitimate interests" condition will not be met if the processing will have a prejudicial effect on the rights and freedoms, or other legitimate interests, of the data subject. Where there is a serious mismatch between competing interests, the subject's legitimate interests should come first. The collecting and processing of data under the legitimate interests condition should be fair and lawful and should comply with all the data protection principles.

Sensitive personal data should only be processed without the individual's explicit consent where it is clearly in the substantial public interest (as authorized by law) or in the vital interests of the data subject (for instance, in a life-threatening emergency).

Timing

As a general rule, an individual should be informed of the purposes at the time the data is collected, and his or her consent should be obtained at that point. In most cases, consent will last for as long as the processing to which it relates continues. In some instances, the subsequent collection of additional data may reasonably be based on the individual's prior consent to the initial collection.

The data subject should be entitled to withdraw his/her consent at any time, for which purpose the controller should establish simple, swift, effective and no-cost mechanisms. In general, withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

[NOTE: Based on article 7.3 of GDPR and Nº 12.2 of the Ibero-American Standards]

THIRD PRINCIPLE: RELEVANCE AND NECESSITY

The data should be relevant and necessary to the stated purposes for which it is collected.

Relevancy and necessity are critical concepts in respect of data protection and personal privacy. Of course, their requirements should be assessed in relation to the specific context in which the personal data is collected, used, and disclosed. Contextual considerations include what particular data is collected and the purposes for which that data is collected.

Relevance

The requirement that data be "relevant" means that it should be reasonably related to the purposes for which it was collected and is intended to be used. For instance, data concerning opinions may easily be misleading if they are used for purposes to which they bear no relation.

Necessity and Proportionality

As a general rule, data processors should only use personal data in ways commensurate with the stated purposes for which the data was collected, for example when necessary to provide the service or product that was requested by the individual. Moreover, data collectors and processors should follow a "limitation" or "minimization" criterion, according to which they should make a reasonable effort to ensure that the personal data handled correspond to the minimum required for the stated purpose. In some legal systems the concept of "proportionality" is used to refer generally to the balancing of competing values. Proportionality requires decision-makers to evaluate whether a measure has gone beyond what is required to attain a legitimate goal and whether its claimed benefits will exceed the anticipated costs.

[Based on article 5.1(c) of GDPR]

In the context of public sector data processing, the idea of necessity is sometimes measured by proportionality, for example to require balancing (i) the public interest in processing the personal data against (ii) protection of the individuals' privacy interests.

Under these Principles, the concepts of "necessity" and "proportionality" place general limitations on use, meaning that personal data should be used only to fulfill the purposes of collection except with the consent of the individual whose personal data is collected or when necessary to provide a service or product requested by the individual.

The Principles recognize, however, that the field of data management and processing is continually evolving technologically. In consequence, this Principle should be understood to embrace a measure of reasonable flexibility and adaptability.

FOURTH PRINCIPLE: LIMITED USE AND RETENTION

Personal data should be kept and used only in a lawful manner not incompatible with the purpose(s) for which it was collected. It should not be kept for longer than necessary for that purpose or purposes and in accordance with relevant domestic law.

This Principle sets forth two fundamental premises regarding retention of personal data: (1) it should be kept and used in a lawful manner not incompatible with the purpose for which they were collected (sometimes referred to as the "principle of purpose" or "purpose limitation") and (2) it should not be kept longer than necessary for that purpose and in accordance with relevant domestic law.

Limited Use

Regarding the first premise, personal data should be collected for specified, explicit and legitimate purposes. Retention and use of personal data should be consistent with individuals' reasonable expectations, their relationship with the data controller collecting the data and the notice(s) provided by the data controller.

[NOTE: Based on article 5.1(b) of GDPR and on Nº 17.1 of the Ibero-American Standards]

Personal data should not be kept or used for purposes other than those compatible with those for which it was collected, except with the knowledge or consent of the data subject or by the authority of law. The concept of "incompatibility" includes a certain measure of flexibility, allowing reference to the overall objective or purpose for which the individual's consent to collection was initially given. In this regard, the appropriate measure may often be one of respecting the context in which the individual had provided his or her personal data and his or her reasonable expectations in the particular situation.

[NOTE: Based on §1798.100(b) of CCPA]

For example, when a data subject provides her name and mailing address to an online retailer, and that retailer in turn discloses that-subject's name and home address to the shipper so that the purchased goods may be delivered to the subject, this disclosure is clearly a "compatible" use of personal data. However, if the online retailer discloses the subject's name and home address to another retailer or marketer for purposes unnecessary for and unrelated to the completion of the subject's online transaction, it would most likely be an "incompatible" use of the consumer's data and not allowed unless the subject offers his/her express consent.

Subsequent processing of personal data for filing or archiving purposes, scientific or historical research purposes or statistical purposes, all in the public interest, shall not be deemed incompatible with the initial purposes.

[NOTE: Based on Nº17.3 of the Ibero-American Standards, article 5.1(b) of GDPR and §1798.140(o)(3)(s) of CCPA]

Thus, another circumstance in which this Principle may be applied reasonably and with a degree of flexibility concerns the use of an individual's personal data as part of a broad (or "aggregate") processing of data from a large number of individuals by the data controller, for example for inventory, statistical or accounting purposes.

Limited Retention

Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. A general limitation on data retention is required by modern technological realities. Because the cost of data storage has been reduced so sharply, it may often be less expensive for data controllers to store data indefinitely rather than to review and delete unnecessary data. Yet unnecessary and excessive retention of personal data clearly has privacy implications. As a general rule, therefore, data should be securely and definitively disposed of —by, for example, deleting them from the controller's information files, records, databases, registers or systems— or should be anonymized, when it is no longer needed for its original purpose or as otherwise required by national law.

[NOTE: Based on article 5.1(d) of GDPR and Nº 19.2 and 19.3 of the Ibero-American Standards]

Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical

purposes, subject to the implementation of the appropriate technical and organizational measures to safeguard the rights and freedoms of the data subject.

[NOTE: Based on article 5.1(e) of GDPR]

Furthermore, individuals may choose to consent, either expressly or by implication, to the use and retention of their personal data for additional purposes. Relevant domestic law may impose explicit legal requirements for data retention. Moreover, a data controller may have legitimate reasons to retain data for a certain period of time even if not explicitly required. For example, employers may retain records on former employees, or doctors may retain records on their former patients, in order to protect themselves against certain types of legal actions, such as medical malpractice, wrongful discharge, etc. It may also be necessary for data controllers to retain personal data for longer periods in order to comply with other legal obligations, or to protect the rights, safety or property of the individual, the data processor, or a third party.

[NOTE: Based on No. 19.4 of the Ibero-American Standards].

FIFTH PRINCIPLE: DUTY OF CONFIDENTIALITY

Personal data should not be disclosed, made available or used for purposes other than those for which it was collected except with the knowledge or consent of the concerned individual or under the authority of law.

This Principle derives from the basic duty of the data controller to maintain the "confidentiality" of personal data in a safe and controlled environment.

This duty requires the data controller to ensure that such data is not given (or otherwise made available) to persons or entities except pursuant to the knowledge, consent or reasonable expectations of the individual concerned or under proper legal authority. The data controller should also ensure that the personal data is not used for purposes which are incompatible with the original purpose for which that data was collected. These responsibilities arise from the nature of the personal data itself and do not depend on assertions by the individuals concerned.

[NOTE: Based on Nº 23 of the Ibero-American Standards]

This duty to respect limits on disclosure is in addition to the obligation of data controllers under the Sixth Principle to promote safety, security, and legal compliance in safeguarding data. Protecting privacy means not only keeping personal data secure, but also enabling individuals to control how their personal data is used and disclosed. An essential element of “informational self-determination” is the establishment and maintenance of trust between data subject and data controller, especially with regard to third-party disclosure of personal data.

In some situations, an individual's consent may reasonably be inferred based on the particular context of the individual’s relationship and interactions with the data controller or its services, the notice(s) provided by the data controller, and commonly accepted practices regarding the collection and use of personal data. For example, in some situations it is entirely reasonable for a data controller to share data with a third party “service provider” (for example, a data processor) under a specified contractual arrangement.

Disclosure to law enforcement authorities and other government agencies pursuant to law would not contravene this Principle but should be authorized by clear and specific provisions.

Protection of personal data in the hands of public authorities may be subject to differing rules depending on the nature of the information and the reasons for disclosure. These reasons and rules should also be addressed by clear and specific provisions. In this regard, attention is drawn to the Model Inter-American Law on Access to Public Information, adopted in 2010, as well as the Draft Model Law 2.0 approved by the IAJC in 2020 that is currently under discussion by the OAS political bodies, which provides that subject entities should protect confidential personal information and particularly personal data whose disclosure requires authorization from the subjects thereof.

SIXTH PRINCIPLE: PROTECTION AND SECURITY

The confidentiality, integrity and availability of personal data should be protected by reasonable and appropriate technical or organizational security safeguards against unauthorized or unlawful processing and against accidental loss, destruction or damage.

Under this Principle, data controllers should take organizational and technical steps to put security safeguards in place that ensure the confidentiality, integrity and availability of personal data in their possession or custody (or for which they are responsible) and to ensure that such personal data is not processed or disclosed except in accordance with the individual's knowledge or consent or other lawful authority, nor is accidentally lost, destroyed or damaged. Accordingly, data controllers should also establish controls or mechanisms to ensure that the confidentiality of the personal data is maintained by processors and any other person involved in the handling of personal data, even after the relation with the data subject comes to an end.

[NOTE: Based on article 5.1(f) of GDPR and Nº 21.1 and 23.1 of the Ibero-American Standards]

Data controllers should provide “reasonable and appropriate security safeguards.” It is based on achieving and maintaining a proper level of care in the context of the overall situation. Thus, considerations of proportionality and necessity may be taken into account.

In the modern context, absolute privacy and complete protection of personal data is technically impossible to guarantee, and the effort to achieve it would impose undesirable barriers and unacceptable costs. Moreover, different contexts may require different solutions and levels of safeguards. Accordingly, this Principle requires an exercise of reasoned and informed judgment and is not necessarily violated any time a data controller experiences an unauthorized access, loss, destruction, damage, use, modification or disclosure.

Personal data should be protected, regardless of the format in which it is held, by safeguards that are reasonably designed to prevent material harm to individuals from the unauthorized access to or loss or destruction of the data. The nature of the safeguards may vary depending on the sensitivity of the data in question.

Clearly, more sensitive data requires a greater level of protection. Reasons for providing enhanced protection might include, for example, the risks of identity theft, financial loss, negative effects to credit ratings, damage to property, loss of employment or business or professional opportunities.

The standard is not static. Threats to privacy, especially cyber threats, are constantly evolving, and the assessment of what are "reasonable and appropriate" safeguards should respond to those developments. The challenge is to provide meaningful guidance to data controllers while ensuring that the standards remain "technologically neutral" and are not rendered obsolete by rapid changes in technology.

Given the rapid rate of change in the current information environment, what might have been permissible practices only a few months ago could well be regarded today as intrusive or risky or dangerous to individual privacy. By the same token, what might have seemed a reasonable restriction a few months ago might in fact be obsolete or unfair in light of technological advances.

The assessment of "reasonable and appropriate security safeguards" should therefore be based on the current "state of the art" in data security methods and techniques in the light of evolving threats to personal privacy. It should also be subject to periodic review and reassessment.

[NOTE: Based on Nº 21.3 of the Ibero-American Standards]

Protecting the privacy of individuals means keeping their personal data secure and enabling them to control their "on-line" experience. In addition to adopting effective security measures, data controllers (such as providers of online services) should have the flexibility to provide their users with effective tools to control the sharing of personal data as part of their overall measures of privacy protection.

Data Breaches

The growing incidence of outside intrusions ("personal data breaches"), in which unauthorized persons gain access to protected data, raises criminal as well as privacy concerns. In many countries, including within our region, domestic law imposes reporting requirements in such instances. Thus, in the event of a breach, data controllers may have a legal obligation to notify the individuals whose data has been (or might have been) compromised.

Such notifications permit the affected individuals to take protective measures and perhaps to access and seek correction of any inaccurate data or misuse resulting from the breaches. The notifications may also provide incentives for data controllers to demonstrate their accountability, to review their data retention policies and to improve their security practices.

At the same time, breach notification laws may impose obligations on data controllers to cooperate with criminal law enforcement agencies as well as other authorities (e.g. computer incident response teams or other entities responsible for cybersecurity oversight). National legislation should determine the specific (and limited) situations in which law enforcement authorities may require the disclosure of personal data without the consent of the individuals concerned. Care should be taken not to impose conflicting notification and/or confidentiality requirements on data controllers.

In cases where penalties are imposed on data controllers for non-compliance with the duty to safeguard and protect, such penalties should be proportional to the level of harm or risk. In this context, it may be useful for national jurisdictions to adopt specific definitions of what constitutes a "breach" (or "unauthorized access"), what types of data may require additional levels of protection in such an event, and what specific responsibilities a data controller may have in the event of such a disclosure.

SEVENTH PRINCIPLE: ACCURACY OF DATA

Personal data should be kept correct, accurate, complete and up-to-date to the extent necessary for the purposes for which it was collected.

Accuracy and precision are vitally important for the protection of privacy. Data accuracy is clearly important to the protection of privacy interests. Inaccurate data can cause harm to both the data processor and the data subject, but to an extent that varies greatly depending on context.

When personal data is collected and retained for continuing use (as distinct from one-time uses or periods of short duration), the data controller should take steps to ensure that the data in its possession is correct, accurate complete and up-to-date, as necessary for the purposes for which it was collected and is being used.

[NOTE: Based on N° 19.1 of the Ibero-American Standards]

The data may or may not need to be continually updated and/or supplemented in order to be accurate in relation to the stated purpose for which the data was collected. In deciding whether additional information is required, the standard should be one of "necessity," that is, the data in question should be accurate, complete and up-to-date to the extent necessary for the purposes of use. The obligation derives from the "use" for which the data was collected and has been or is intended to be put, and for which the individual has given consent. It is not an abstract requirement of objective accuracy. Therefore, the data controller or data controllers should adopt appropriate mechanisms – reasonable in light of the purpose for which the date was collected and is used – to make sure that the data remains correct, accurate, complete and up-to-date, and that the rights of the individual in question are not impaired.

Data controllers should undertake effective efforts to safeguard the privacy of individuals and others who provide their own data. Data controllers may satisfy their obligations with regard to accuracy by providing individuals with a reasonable opportunity to review, correct or request deletion of personal information they have provided to the data controller. The requirement may be subject to a reasonable time limitation.

In taking measures to determine the accuracy of individuals' personal data ("data quality"), the data controller may consider the sensitivity of the personal data that they collect or maintain and the likelihood it may expose individuals to material harm, consistent with the requirements of the Ninth Principle.

As mentioned under the Third and Fourth Principles above, as per the 'minimization' and limited use and retention criteria, personal data handled should correspond to the minimum required for the stated purpose and should not be kept for longer than necessary for the purposes stated. In many situations, the application of this Principle will require the deletion of personal data which is no longer necessary for the purposes which initially justified its collection.

In limited circumstances (for example, the investigation of or protection against fraud), data processors may need to retain and process some inaccurate or fraudulent data.

EIGHTH PRINCIPLE: ACCESS, RECTIFICATION, ERASURE, OBJECTION AND PORTABILITY

Reasonable methods should be available to permit individuals whose personal data has been collected the rights to access, obtain rectification, and obtain erasure of personal data regarding them, as well as the right to object to its processing and, where applicable, the right to data portability thereof. As a general rule, the exercise of such rights should be free of cost. Should it be necessary to curtail the scope of these rights, the specific grounds for any such restrictions should be specified in domestic law.

[NOTE: Based on Chapter III of the Ibero-American Standards]

Individuals should have the right to discover whether data controllers have personal data relating to those individuals, to have access to that data so that they may challenge the accuracy of that data, and

to ask the data controller to amend, revise, correct or delete the data in question. This right of access and rectification is one the most important safeguards in the field of privacy protection. They should also have the right to obtain erasure of the personal data and to object to its processing. Where applicable, they also have the right to data portability.

The essential elements are the individual's ability to obtain data relating to him or her within a reasonable time, and in a reasonable and intelligible manner; to know whether a request for such data has been denied and why; and to challenge such a denial. As a general rule, the exercise of these rights should be free of cost; exceptionally, costs should be only those naturally inherent to the reproduction, delivery or certification of the data.

[NOTE: Based on preambular paragraph 19 of the Ibero-American Standards; paragraph 1798.100(d) of the CCPA]

Within the Western Hemisphere, some (but not all) national legal systems recognize a right of *habeas data*, by which individuals are able to file a judicial proceeding to prevent or terminate an alleged abuse of their personal data. That right may provide the individual access to public or private data bases, the right to correct the data in question, to ensure that sensitive personal data remains confidential, and to rectify or remove damaging data. Because the specific contours of this right vary between Member States, these Principles address the issues it raises in terms of its separate elements.

The national legislation of each State should establish the requirements, periods, deadlines, terms and conditions under which data subjects may exercise their rights of access, rectification, erasure~~,~~ objection and portability. These rights are not absolute and national legislation should clearly state the causes and reasons for which the exercise of such rights may be impeded. These may include, among others, 1) when processing is necessary in order to pursue an important objective in the public interest or for the exercise of their specific functions by public authorities; 2) when the controller believes that it has lawful reason for the processing to prevail over the interests, rights and freedoms of the subject; 3) when processing is needed in order to comply with a legal provision; or 4) when the personal data is needed to ensure compliance with a legal or contractual relationship.

Should the data subject be deceased or have disappeared, the national legislation of each State may allow natural persons who are their legal representatives or relatives to exercise these rights regarding the personal data of such subjects.

National legislation of each State may also recognize the right of the data subject to disagree with or contest the controller's response or lack of response to a request to exercise the rights addressed in this Principle before the control authority and, as applicable, before a judicial court in accordance with the domestic law of each State.

[NOTE: Based on N°s 32.3 and 32.4 of the Ibero-American Standards]

Data controllers and data processors should not discriminate against data subjects because they exercised any of these rights, including but not limited by denying goods or services to the subject, charging different prices or rates for them or providing them a different level or quality of goods.

[NOTE: Based on §1798.125 of the CCPA]

The Right of Access

The right to access personal data held by a data controller should be simple to exercise. For example, the mechanisms for access should be part of the routine activities of the data controller and

should not require any special measures or legal process (including, for instance, presenting a formal judicial claim). Every individual should have the ability to access his or her own data. In some situations, even third parties may also be entitled (for example, representatives on behalf of those suffering mental incapacity, or parents on behalf of minor children).

The ability of an individual to seek access to his or her data is sometimes referred to as the right of "individual participation." Under this concept, access should be afforded within a reasonable time period, a reasonable manner and in a reasonably intelligible form. As mentioned, access should be afforded free of cost; exceptionally, costs should be only those naturally inherent to the reproduction, delivery or certification of the data. The burden and expense of producing the data should never be unreasonable or disproportionate.

[NOTE: Based on preambular paragraph 19 of the Ibero-American Standards; paragraph 1798.100(d) of the CCPA]

Any data to be furnished to the data subject should be provided in an intelligible form, using a clear and simple language. The information may be delivered by mail or electronically, and if provided electronically it should be portable as described below *(cf.* section 'Right to Personal Data Portability', *infra*).

[NOTE: Based on preambular paragraph 19 and paragraph 25 of the Ibero-American Standards; article 15 of GDPR; paragraph 1798.100(d) of the CCPA]

Exceptions and Limitations

The right of access is not absolute, however. Some exceptional situations exist in every national scheme which may require certain data to be kept confidential. These circumstances should be clearly set out in the appropriate legislation or other guidance and should be available to the public.

Such situations may arise, for example, where the individual concerned is suspected of wrongdoing and is the subject of an ongoing law enforcement or similar investigation, or where that individual's records are intermingled with those of a third party who also has privacy interests, or where granting the data subject access would compromise trade secrets or confidential testing or examination material. The rules regarding such situations should be as narrow and restrictive as possible.

In addition, for practical reasons, a data controller may impose reasonable conditions, for example by specifying the method by which requests should be made and by requiring the individuals making such requests to authenticate their identity through reasonable means. Data controllers need not accede to requests that would impose disproportionate burdens or expenses, violate the privacy rights of other individuals, infringe on proprietary data or business secrets, contravene the data controllers' legal obligations, or otherwise prevent the company from protecting the rights, safety or property of the company, another user, an affiliate, or a third party.

The Right to Challenge Denial of Access

In the event that an individual's request for access is denied, there should be an effective method by which the individual (or her representative) can learn the reasons for the denial and challenge that denial. Allowing the individual to learn the reasons for an adverse decision is necessary for the exercise of the right to challenge the decision and to prevent arbitrary denials.

As indicated above, it may well be appropriate, or even necessary, in some situations to withhold certain data. Such situations should however be the exception, not the rule, and the reasons for the denial

should be clearly communicated to the individual making the request, in order to prevent arbitrary denial of the fundamental right to correct errors and mistakes.

The Right to Rectify Errors and Omissions

The individual should be able to exercise the right to request the correction of (or an addition to) personal data about himself or herself that is incomplete, inaccurate, unnecessary, excessive or not up-to-date. This is sometimes referred to as the right of "rectification." When the data in question is incomplete or inaccurate, the individual should be permitted to provide additional information to correct those errors or omissions.

Where the data in question is clearly inaccurate, the data controller should generally correct the inaccuracy when the data subject so requests. Even where data has been found to be inaccurate, such as in the course of an investigation involving the data subject, it may be more appropriate in some situations for the data controller to add additional material to the record rather than deleting it, so as to accurately reflect the entire investigative history.

The data subject should not be allowed to inject inaccurate or erroneous data into the data controller's records. The data subject also does not necessarily have a right to compel the data controller to delete data that is accurate but embarrassing.

The right of correction or rectification is not absolute. For example, amendment of personal data – even erroneous or misleading information - may not be authorized where that data is legally required or should be retained for the performance of an obligation imposed on the responsible person by the applicable national legislation, or possibly by the contractual relations between the responsible person and the data subject.

Accordingly, national legislation should clearly indicate the conditions under which access and correction should be provided and the restrictions that apply. It should specify the limited situations in which personal data may not be accessible and cannot be corrected. The specific grounds for such restrictions should be clearly specified.

Right to erasure

Some national and regional regulatory schemes provide individuals with a right to request that data controllers delete (or erase) specific personal data which, although publicly available, the individuals contend is no longer necessary or relevant or regarding which the data subject withdraws its consent or objects to its processing. This right is sometimes described as the right to omit or suppress specific information, to "de-identification" or "anonymization." Where the right to erasure is recognized, and upon receipt of a request thereto, data controllers should proceed to delete the personal data from their records and should also direct any data processors to delete the subject's personal data from their records.

[Note: Based on art. 17 of GDPR, No. 27 of the Ibero-American Standards and §1798.105 of the CCPA]

The right is not absolute but rather contingent and contextual, and it requires a difficult and delicate balancing of interests and principles. Exercise of the right necessarily presents fundamental issues not just about privacy, honor and dignity, but also about the rights of access to truth, freedom of information and speech, and proportionality. Exceptions to the exercise of the right of erasure should be clearly established in domestic laws, and may include, for example, cases where the data is necessary to complete the transaction for which the personal data was collected, fulfill the terms of a written warranty

or product recall conducted in accordance with law, perform a contract, detect security incidents, protect against malicious, deceptive, fraudulent or illegal activity, debug to identify and repair errors, exercise free speech or engage in scientific, historical or statistical research in the public interest, among others.

[Note: Based on §1798.105 of the CCPA]

In some States, the "right to erasure or deletion" remains contentious and subject to differing definitions and views regarding personal data which (while true or factually accurate) is considered personally embarrassing, excessive or merely irrelevant by the individual concerned.

Right to Object

Data subjects should have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her when endowed with a legitimate interest thereto or when the processing thereof is for direct marketing purposes, which includes profiling to the extent that is related to such direct marketing. When the data subject objects to processing for direct marketing purposes, the personal data should no longer be processed for such purposes.

[Note: Based on article 21 of GDPR and No. 28 of the Ibero-American Standards]

Right to Personal Data Portability

When personal data is processed electronically or through automated means, the data subject should have the right to receive the personal data concerning him or her, which he or she has provided to a controller–in a structured, commonly used and machine-readable format, and which allows the ongoing use and transfer thereof to another controller without hindrance, if desired.

[NOTE: Based on preambular paragraph 19 of the Ibero-American Standards; article 20 of GDPR; paragraph 1798.100(d) of the CCPA;]

The subject may ask for his/her personal data to be transferred directly from controller to controller, when this is technically possible. The right to personal data portability should have no negative effects on the rights and freedoms of others.

Without adversely affecting other rights of the subject, the right to data portability should not be justified when involving information that is inferred, derived, created, generated or obtained from processing or analyses conducted by the controller on the basis of the personal data provided by said subject, as occurs ,for example, with the personal data that has been run through a personalization, recommendation, categorization or profile creation process.

[Note: based on article 30.4 of the Ibero-American Standards and article 20 of GDPR]

NINTH PRINCIPLE: SENSITIVE PERSONAL DATA

Some types of personal data, given its sensitivity in particular contexts, are especially likely to cause material harm to individuals if misused. Data controllers should adopt privacy and security measures that are commensurate with the sensitivity of the data and its capacity to harm individual data subjects.

The term "sensitive personal data" refers to data regarding the most intimate aspects of individuals. Depending on the specific cultural, social or political context, it might include, for example, data related to an individual's personal health, sex life or sexual preferences, religious, philosophical or moral beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, political opinion or racial or ethnic origins.

[NOTE: Based on N° 2.1 (d) of the Ibero-American Standards, article 9 of GDPR and article 4.2 of the OECD Decision]

In certain circumstances, this data might be considered worthy of special protection because its improper handling or disclosure would intrude deeply upon the personal dignity and honor of the individual concerned and could trigger unlawful or arbitrary discrimination against the individual or result in risk of serious harm to the individual.

Accordingly, appropriate guarantees should be established within the context of national law and rules to ensure that the privacy interests of individuals are sufficiently protected. Member States should identify clearly the categories of personal data which are considered especially "sensitive" and therefore require enhanced protection, as well as the scope of the prohibition of their processing and the exceptions thereto. As a general rule, sensitive personal data should not be processed except, for example, when the data subject has provided explicit consent thereto or when processing is strictly necessary for the purposes of carrying out the obligations and exercising specific rights of the data controller, or is necessary to comply with a legal mandate, or is necessary for reasons of national security, public safety, public order, public health or the safeguard of rights and freedoms of third parties. The context in which a person provides such data should be taken into account when determining any applicable regulatory obligations.

[Note: Based on No. 9 of the Ibero-American Standards and article 9 of GDPR]

The burden should be placed on data controllers to assess the material risks to data subjects as part of the overall process of risk management and privacy impact assessment. Holding data controllers accountable will result in more meaningful protection of data subjects from material harm across a wide range of cultural contexts.

[Note: Based on No 9 of the Ibero-American Standards]

TENTH PRINCIPLE: ACCOUNTABILITY

Data controllers should adopt and implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with these Principles. The data controller and processor and, where applicable, their representatives, should cooperate, on request, with the data processing authority in the performance of their tasks.

[NOTE: Based on N° 20.1 of the Ibero-American Standards and articles 24 and 31 of GDPR].

The effective protection of individual rights of privacy and data protection rests on responsible conduct by the data controllers as much as it does on the individuals and government authorities concerned. Privacy protection schemes should reflect an appropriate balance between government regulation and effective implementation by those with direct responsibility for the collection, use, retention and dissemination of personal data.

These Principles depend on the ability of those who collect, process and retain personal data to make responsible, ethical, and disciplined decisions about that data and its use through the data's "lifecycle." These "data managers" should serve as "good stewards" of the data provided or entrusted to them.

Accountability

The principle of accountability requires establishing and adhering to appropriate privacy protection goals for data controllers (organizations and other entities), permitting them to determine the most appropriate measures to reach those goals, and monitoring their compliance. It enables data

controllers to achieve those privacy protection goals in a manner that best serves their business models, technologies, and the requirements of their customers.

Data controllers should implement appropriate technical and organizational measures to ensure and to be able to demonstrate, upon request, that processing is performed in accordance with these Principles. When processing is to be carried out on behalf of a controller, the controller should use only processors providing sufficient guarantees to implement technical and organizational measures in such a manner that processing will meet these Principles and ensure the protection of the rights of the data subject.

[Note: Based on articles 24 and 28 of the GDPR and No. 20 of the Ibero-American Standards, and article 6.1 of the OECD Decision]

Specific programs and procedures should take into account the nature of the personal data at issue, the size and complexity of the organization which collects, stores and processes that data, and the risk of violations. Privacy protection depends upon a credible assessment of the risks the use of personal data may raise for individuals and responsible mitigation of those risks. Appropriate resources should be destined for the implementation of data protection programs, policies and procedures, which should include, among others, risk management systems, training on data protection obligations, periodic review of security programs, a system of supervision and surveillance, including audits, to assess the compliance of data protection policies, as well as procedures to receive and respond to questions and complaints by data subjects. Adherence to codes of conduct or certification mechanisms, among others, may be used as elements by which to demonstrate compliance with these Principles.

[Based on No. 20.1 to 20.3 of the Ibero-American Standards and article 24 of GDPR]

National privacy legislation and regulation should therefore provide clearly articulated and well-defined guidance for use by data controllers. It should encourage the development of self-regulatory codes of conduct that keep pace with technological developments and that account for privacy principles and regulations in other jurisdictions.

Data controllers should ensure that employees who handle personal data are appropriately trained about the purposes and procedures for the protection of that data. They should adopt effective privacy management programs and conduct internal reviews designed to promote the privacy of individuals. In many cases, the designation of a “chief information and privacy official” will assist in achieving this goal.

Above all, national privacy legislation should hold data controllers accountable for compliance with these Principles. In addition to whatever enforcement mechanism may be available to governmental authorities, domestic law should provide individuals with appropriate mechanisms for holding data controllers liable for violations (for example, through civil damages).

Privacy by Design

One effective contemporary approach is to require data controllers to build privacy protection into the design and architecture of their information technology systems and business practices. Privacy and security considerations should be incorporated into every stage of product design.

Data controllers should be prepared to demonstrate their privacy management programs when asked, in particular at the request of a competent data protection authority or another entity responsible for promoting adherence to a code of conduct.

Based on No. 20 of the Ibero-American Standards, articles 24 and 31 of GDPR and article 6.1 of the OECD Decision]

Sharing Personal Data with Third Parties

Data sharing and retransmission is a growing practice among data controllers. It presents some difficult issues. At a minimum, however, an individual's consent to the initial collection of personal data does not automatically authorize the sharing (or retransmission) of that data to other data controllers or data processors. Individuals should be informed about, and given appropriate opportunities to consent to, such additional sharing.

These Principles indicate that data controllers should be held responsible for ensuring that their requirements are observed by any third party to whom the personal data is communicated. This obligation to ensure adequate security safeguards applies whether or not it is another person in charge or a different data controller handling personal data on behalf of the responsible (accountable) authority. It also applies in the case of international or trans-border transfers of personal data (see Principle Eleven).

ELEVENTH PRINCIPLE: TRANS-BORDER FLOW OF DATA AND ACCOUNTABILITY

Member States should cooperate with one another in developing mechanisms and procedures to ensure that data controllers and processors operating in more than one jurisdiction can be effectively held accountable for their adherence to these Principles.

In the modern world of rapid data flows and cross-border commerce, personal data is increasingly likely to be transferred across national boundaries. However, the rules and regulations in various national jurisdictions today differ in substance and procedure. In consequence, the possibility exists for confusion, conflict and contradictions.

One central challenge for effective data protection policy and practice is to reconcile (i) the differences in national approaches to privacy protection with the modern realities of global data flow, (ii) the rights of individuals to access data in a transnational context, and (iii) the fundamental fact that data and data processing drive development and innovation. All international data protection instruments strive towards achieving the proper balance between these goals.

These Principles articulate a common standard for evaluating privacy protections within OAS Member States. The fundamental goal is harmonization of regulatory approaches that provide more effective privacy protection while promoting safe data flows for economic growth and development. In point of fact, not every OAS Member State today provides precisely the same protections.

In common with other international standards in this field, these Principles adopt a standard of reasonableness with respect to cross-border transfers. On the one hand, international transfers of personal data should be permitted between Member States which afford the levels of protection reflected in these Principles or which otherwise provide sufficient protection for personal data, including effective enforcement mechanisms. At the same time, transfers should also be permitted when data controllers themselves take appropriate measures to ensure that transferred data is effectively protected in accordance with these Principles. Member States should take the necessary measures to ensure that data controllers and processors are held accountable for providing such protection.

Trans-Border Personal Data Flows

Transfer of personal data across national borders is a fact of contemporary life. Our global community is more inter-connected than ever. In most countries, information from all parts of the world is readily available to anyone with a keyboard and internet connection. International law recognizes the right of individuals to privacy and the protection of personal data aligned with the free flow of

information. Equally important, domestic economies are increasingly dependent on trans-border trade and commerce, and the transfer of data (including personal data) is a fundamental aspect of that trade and commerce.

As new technologies emerge, storage of data is becoming geographically indeterminate. So-called "cloud" computing and storage, and the increasing prevalence of mobile services, necessarily involve the exchange and remote storage of data across national boundaries. A progressive approach to privacy and security should permit domestic enterprises and industries to grow and compete internationally. Unnecessary or unreasonable national restrictions on cross-border data flows have the potential to create barriers to trade in services and to hinder development of products and services that are innovative, efficient and cost effective. They can easily become obstacles to exports and do considerable harm to service providers as well as to individuals and business customers. Restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing. Any such restrictions should be non-discriminatory.

OAS Member States are encouraged to consider the recognition of interoperable standards for trans-border transfers in order to facilitate the unrestricted flow of data between Member States with disparate scopes and stages of development of their domestic data privacy laws. This would enable shared accountability and cooperation between these States in the event of unauthorized transfers, and would contribute to increase trade, investment and economic outcomes for Member States' economies, as well as spur innovation and lower barriers to entry to the global economy.

[Based on APEC CBPR framework, USMCA art. 19.3]

National Restrictions Based on Differing Levels of Protection

Within the OAS, all Member States share the overall goal of protecting privacy as well as a commitment to the free flow of information within certain criteria. Member States should refrain from restricting data flows to other States that are substantially observing these Principles, or where appropriate safeguards are present. A majority of countries around the globe do likewise. Nonetheless, in some countries, authorities have imposed restrictions on the trans-border communication of data by individuals and entities subject to their jurisdiction when, in the opinion of those authorities, the data protection rules in the other countries falls short of the specific requirements of the authorities' own law. For example, an entity in country A may be prevented from communicating data to an entity in country B if, in the opinion of A's authorities, the privacy or data protection laws in B fails to meet A's standards – even if both entities are part of the same commercial organization.

In particular (limited) circumstances, national law may justifiably restrict the trans-national data flow and may require data to be stored and processed locally. The reasons for restricting or preventing data flows should always be compelling. Some reasons for such restrictions may be more compelling than others. As a general matter, however, "data localization" requirements are inherently counter-productive and should be avoided, in favor of cooperative measures. .

While motivated by privacy protection concerns, such restrictions can amount to an extraterritorial application of domestic law and (if unduly rigorous) may impose unnecessary and counterproductive barriers to commerce and development, harmful to the interests of the jurisdictions concerned.

International cooperation

For these reasons, the principles and mechanisms of international cooperation should work to limit and reduce friction and conflict between different domestic legal approaches governing the use and transfer of personal data. Mutual respect for the requirements of other countries' rules (including their

privacy safeguards) will foster cross-border trade in services. In turn, such respect should rest on a concept of transparency between Member countries in respect of requirements and procedures for the protection of personal data.

Member States should work towards mutual recognition of accountability rules and practices, in order to avoid and resolve conflicts. Member States should promote the cross-border transfer of data (subject to appropriate safeguards) and they should not impose burdens that limit the free flow of information or economic activity between jurisdictions, such as requiring service providers to operate locally or to locate their infrastructure or data within a country's borders. National legislation should not inhibit access by data controllers or individuals to information that is stored outside of the country as long as that information is given levels of protection that meet the standards provided herein.

Accountability of Data Controllers

Data controllers should of course be expected to comply with legal obligations in the jurisdiction where they maintain their principal place of business and where they operate.

At the same time, data controllers transferring personal data across borders should themselves assume responsibility for assuring a continuing level of protection consistent with these Principles.

Data controllers should take reasonable measures to ensure personal data is effectively protected in accordance with these Principles, whether the data is transferred to third parties domestically or across international boundaries. They should also provide the individuals concerned with appropriate notice of such transfers, specifying the purposes for which the data will be used by those third parties. In general, such obligations should be recognized in appropriate agreements or contractual provisions or through technical and organizational security safeguards, complaint handling processes, audits, and similar measures. The idea is to facilitate the necessary flow of personal data between Member States while, at the same time, guaranteeing the fundamental right of individuals to protection of their personal data.

These Principles may serve as an agreed-upon framework for enhanced cooperation and capacity-building efforts between privacy enforcement authorities in the OAS Member States based upon common standards for assuring the basic requirements of trans-border accountability.

TWELFTH PRINCIPLE: EXCEPTIONS

When national authorities make exceptions to these Principles for reasons relating to national sovereignty, national security, public security, protection of public health, the fight against criminality, regulatory compliance or other public order policies, the protection of rights and freedoms of others, or public interest, they should establish them specifically by law or norm and make those exceptions known to the public.

[NOTE: Based on Nº 6 of the Ibero-American Standards and article 23 of GDPR]

Protecting the privacy interests of individuals (citizens and others) is increasingly important in a world in which data about individuals is widely collected, rapidly disseminated, and stored for long periods of time. These Principles aim at providing individuals with the basic rights needed to safeguard their interests.

Yet privacy is not the only interest which Member States and their governments should take into account in the field of data collection, retention and dissemination. On occasion, other responsibilities

of the State will inevitably need to be taken into account and may operate to limit the privacy rights of individuals.

In some situations, authorities in OAS Member States may be required to derogate from, or make exceptions to, these Principles for reasons related to overriding concerns of national security and public safety, the protection of public health, the administration of justice, regulatory compliance, the protection of rights and freedoms of others, or other essential public policy prerogatives or objectives of general public interest. For example, in responding to the threats posed by international crime, terrorism and corruption, and certain severe human rights violations, the competent authorities of OAS Member States have already made special arrangements for international cooperation regarding the detection, investigation, punishment and prevention of criminal offenses.

[NOTE: Based on Nº 6 of the Ibero-American Standards and article 23 of GDPR]

Such exceptions and derogations should be the exception, not the rule. They should only be implemented after the most careful consideration of the importance of protecting individual privacy, dignity and honor. National authorities should maintain sensible limitations on their ability to compel data controllers to disclose personal data, balancing the need for the data in limited circumstances and due respect for the privacy interests of individuals.

Member States should, by public legislation or regulation, clearly identify these exceptions and derogations, indicating the specific situations in which data controllers may be required to disclose personal data and the reasons therefore. They should permit data controllers to publish relevant statistical information in the aggregate (for instance, the number and nature of government demands for personal data) as part of the overall effort to promote effective protection of privacy. They should also disclose this data promptly and publicly.

THIRTEENTH PRINCIPLE
DATA PROTECTION AUTHORITIES

Member States should establish independent supervisory bodies, in accordance with each State's constitutional, organizational and administrative structure, to monitor and promote the protection of personal data in consistency with these Principles.

Most of the OAS Member States have established national autonomous regulatory bodies for setting and enforcing the laws, regulations, and requirements relating to the protection of personal data to ensure consistency across the country. In other Member States, various governmental levels (national, regional, municipal) have each created their own data protection rules and authorities. In still others, the regulatory schemes might differ according to the sector or field of activity (banking, medical, educational, etc.), and responsibility might be shared between regulatory bodies and private entities which are subject to specific legal responsibilities.

Because no uniform approach is reflected in the region, each of the OAS Member States should individually address the specific nature, structure, authorities and responsibilities of these "data protection authorities."

Member States are encouraged to establish appropriate and effective legal, administrative and other provisions, procedures or institutions to ensure the protection of privacy and individual liberties in respect of personal data. They should create reasonable means for individuals to exercise their rights and should encourage and support self-regulation (in the form of codes of conduct or otherwise) for data

controllers and data processors. They should also provide for adequate sanctions and remedies in case of failures to comply and ensure that there is no unfair discrimination against data subjects.

Member States should also set the minimum requirements for the kind of data protection authorities they may choose to establish, in order to provide the necessary resources, funding and technical expertise that will enable said agency to discharge their functions effectively.

ANNEX

Part I. Right to Privacy

As indicated in the text, provisions on privacy, protection of personal honor and dignity, freedom of expression and association, and the free flow of information are found in all the major human rights systems of the world.

For example, the concept of privacy is clearly established in Article V of the American Declaration of the Rights and Duties of Man (1948) as well as Article 11 of the American Convention on Human Rights ("Pact of San Jose") (1969). [3]

Article V of the American Declaration of the Rights and Duties of Man provides:

> Every person has the right to the protection of the law against abusive attacks upon his honor, his reputation, and his private and family life.

See also Article IX ("Every person has the right to the inviolability of his home") and Article X ("Every person has the right to the inviolability and transmission of his correspondence").

Article 11 of the American Convention on Human Rights provides:

> 1. Everyone has the right to have his honor respected and his dignity recognized.
>
> 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.
>
> 3. Everyone has the right to the protection of the law against such interference or attacks. [4]

European Charter

Only the Charter of Fundamental Rights of the European Union (adopted 2000) specifically addresses privacy in the context of data protection.

Article 8 of that Charter provides:

> (1) that everyone has the right to the protection of personal data related thereto,
>
> (2) that such data should be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law, and that everyone has the right of access to data which has been collected related thereto, and the right to have it rectified, and
>
> (3) compliance with these rules shall be subject to control by an independent authority.

The EU Charter thus appears to distinguish data protection from the right to respect for private and family life (art. 7), freedom of thought, conscience and religion (art. 10), and freedom of expression

---

[3] See also the Universal Declaration of Human Rights (arts. 12, 18-20), the International Covenant on Civil and Political Rights (arts. 17-19), the European Convention on Human Rights and Fundamental Freedoms (arts. 8-10), the Charter of Fundamental Freedoms of the European Union (arts. 1, 7, 8, 10-12), and the African Charter of Human and Peoples' Rights (arts. 5, 8-11 and 28).

[4] In addition, Article 14 of the American Convention ("Right of Reply") provides:

> 1. Anyone injured by inaccurate or offensive statements or ideas disseminated to the public in general by a legally regulated medium of communication has the right to reply or to make a correction using the same communications outlet, under such conditions as the law may establish.
> 2. The correction or reply shall not in any case remit other legal liabilities that may have been incurred.
> 3. For the effective protection of honor and reputation, every publisher, and every newspaper, motion picture, radio, and television company, shall have a person responsible who is not protected by immunities or special privileges.

and information (art. 11). Scholars continue to debate whether an independent right to protection of personal information does exist, or is instead properly considered part of a more general right to privacy.[5]

Part II. The Right to Free Flow of Information

Article IV of the American Declaration of the Rights and Duties of Man provides:

> Every person has the right to freedom of investigation, of opinion, and of the expression and dissemination of ideas, by any medium whatsoever.

Article 13 of the American Convention on Human Rights provides:

> 1. Everyone has the right to freedom of thought and expression. This right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice.
> 2. The exercise of the right provided for in the foregoing paragraph shall not be subject to prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure:
>
> a. respect for the rights or reputations of others; or
>
> b. the protection of national security, public order, or public health or morals.
>
> 3. The right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions.
> 4. Notwithstanding the provisions of paragraph 2 above, public entertainments may be subject by law to prior censorship for the sole purpose of regulating access to them for the moral protection of childhood and adolescence.
> 5. Any propaganda for war and any advocacy of national, racial, or religious hatred that constitute incitements to lawless violence or to any other similar action against any person or group of persons on any grounds including those of race, color, religion, language, or national origin shall be considered as offenses punishable by law.

Article 19 of the Universal Declaration of Human Rights (1948) states:

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

Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (entitled "Freedom of Expression") provides:

> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

[5] See for example Orla Lynskey, "Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order," 63 Int'l & Comp. Law Q. 569 (2014).

The World Summit on the Information Society's 2003 Declaration of Principles (paras. 24-26) (available at *http://www.itu.int/wsis/docs/geneva/official/dop.html)* emphasized that:

> The ability for all to access and contribute information, ideas and knowledge is essential in an inclusive Information Society.
>
> The sharing and strengthening of global knowledge for development can be enhanced by removing barriers to equitable access to information for economic, social, political, health, cultural, educational, and scientific activities and by facilitating access to public domain information, including by universal design and the use of assistive technologies.
>
> A rich public domain is an essential element for the growth of the Information Society, creating multiple benefits such as an educated public, new jobs, innovation, business opportunities, and the advancement of sciences. Information in the public domain should be easily accessible to support the Information Society, and protected from misappropriation. Public institutions such as libraries and archives, museums, cultural collections and other community-based access points should be strengthened so as to promote the preservation of documentary records and free and equitable access to information.

Part III. Appended Texts on Data Privacy and Protection

The following includes a selection of the texts most likely to be useful to legislators and other governmental authorities.

- OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data (1980, as revised in 2013)
- The Madrid Resolution: International Standards on the Protection of Personal Data and Privacy (2009)
- The APEC Privacy Framework (2004)
- APEC Cooperation arrangement for Cross-Border Privacy Enforcement
- EU Directive 2002/58/EC on privacy and electronic communications (July 12, 2002)
- EU Directive 95/6/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Oct. 24, 1995)
- COE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108, Jan. 28, 1981) and Protocol (2001)
- UN Guidelines for the Regulation of Computerized Data Files (1990)
- AU Convention on Cyber Security and Personal Data (adopted June 27, 2014)

* * *