STANDARDS FOR PERSONAL DATA

PROTECTION FOR IBERO-AMERICAN STATES

RED IBEROAMERICANA DE PROTECCION DE DATOS

JUNE 20, 2017

STANDARDS FOR
PERSONAL DATA PROTECTION
FOR IBERO-AMERICAN STATES

The Ibero-American Data Protection Network (RIPD, after its acronym in Spanish, or simply Network), within the framework of the XV Ibero-American Data Protection Meeting, has officially approved and presented the so-called 'Data Protection Standards of the Ibero-American States'. This fulfils both a longed-for desire of all the member entities and one of the agreements adopted at the XXV Ibero-American Summit of Heads of State and Government. The Summit, held on October 28 - 29, 2016, in Colombia, agreed to request the elaboration of a proposal aiming at the effective cooperation related to the protection of personal data and privacy from the Network.

The approved text attempts to respond to one of the pillars of the strategy agreed by the RIPD in November 2016 in Montevideo, which is reflected in the RIPD 2020 document: "the aim is to promote and contribute to the strengthening and adaptation of regulatory processes in the region, through the elaboration of guidelines that serve as a parameter for future regulations or for the revision of existing ones".

In this sense, the Ibero-American Standards constitute a set of guidelines that may contribute to the issuance of regulatory initiatives for the protection of personal data in the Ibero-American region, which encompasses those countries that do not have these regulations yet; or, if it were the case, they may serve as reference for the modernization and updating of existing legislation.

The following are some of the objectives of the Ibero-American Standards:

- To establish a set of common principles and rights for the protection of personal data which could be adopted by the Ibero-American States and develop their national legislation thereon, with the goal of having homogenous rules in the region.

- To guarantee the effective exercise and guardianship of the right to the protection of personal data of any person in the Ibero-American States, by establishing common rules that ensure due treatment of their personal data.

- To make the flow of personal data between Ibero-American States and beyond their borders easier, in order to contribute to the economic and social growth of the region.

- To foster international cooperation amongst controlling authorities of the Ibero-American States, with other non-regional controlling authorities, and with international authorities and agencies in this field.

The adoption of the Guidelines for Harmonization of Data Protection in the Ibero-American Community by the RIPD itself, in 2007, on occasion of the V Ibero-American Data Protection Meeting, can be mentioned as one direct antecedent of these Standards. Then, with the adoption of the Guidelines, a 'harmonized framework' of reference for the national regulatory initiatives that arose in the region in data protection matters was established. On the other hand, there are also the standards approved at the International Conference of Data Protection and Privacy Authorities in Madrid in 2009, the so-called "Madrid Standards", which undoubtedly constituted progress in the search for solutions and specific provisions "that could be applied regardless of differences between existing models of data protection and privacy".

Other international and emblematic instruments for the protection of personal data have also been taken as reference for the elaboration of the Ibero-American Standards. As examples, we can mention the Guidelines for the Protection of Privacy and the Transboundary Movement of Personal Data of the Organization for Economic Cooperation and Development (OECD); the Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data and its Protocol; The Privacy Framework of the Asia-Pacific Economic Cooperation Forum; and the Regulation of the European Parliament and Council on the protection of individuals with regard to the processing of personal data and the free movement of such data.

The route followed for the elaboration of these Standards comprised the following stages:

- June, 2016: the XIV Ibero-American Meeting on Data Protection, held on June 8, 2016 in Santa Marta, Colombia, agreed that the National Institute of Transparency, Access to Information and Protection of Personal Data (INAI), would prepare the Ibero-American Standards in its capacity as president of the Network at the time.

- November, 2016: INAI presented the preliminary draft of Ibero-American Standards to the members attending the Network at the RIPD Seminar at the Centre for Spanish Cooperation in Montevideo, held on 8 and 9 November in Uruguay. It was agreed during the Seminar that the preliminary draft of the Ibero-American Standards would be open for comments and observations from the members of the Network throughout the month of December, 2016.

- May, 2017: The resulting version of the Standards, after the contributions received during December 2016, was studied and debated from a technical point of view in the RIPD Workshop at the Centre of Spanish Cooperation in Cartagena de Indias. The workshop was attended by member authorities of the RIPD, a representative of the European Data Protection Supervisor and the Organization of American States, as well as by European Commission's International Flows Unit, by means of videoconference.

- June, 2017: This last version, after the work done during the RIPD Workshop, was unanimously approved in the closed session of the Meeting of Cartagena de Indias at the XV Ibero-American Data Protection Meeting, held from June 20 to 22, 2017 in Santiago, Chile. It was formally proclaimed in the Open Session.

With the approval of these Standards, the RIPD has an essential tool to rigorously address the follow-up and support of future legislative developments in the Region, since the Ibero-American Standards are a normative model that:

- Responds to the national and international needs and demands required by the right to personal data protection, in a society where information and knowledge technologies become increasingly important in all the tasks of everyday life.

- Includes the best national and international practices in this area.

- Proposes a series of standards flexible enough to facilitate their adoption among the Ibero-American States, without in any way contravening their domestic law, in such a way that this document is a living and viable reality in the Ibero-American region which benefits the holders.

- Guarantees an adequate level of protection of personal data in the Ibero-American region, with the aim of establishing no barriers to their free circulation within the Ibero-American States and, consequently, favouring commercial activities between the region, as well as with other Economic regions.

On the other hand, and not any less importantly, the Ibero-American Standards will allow for the reinforcement of the position of the Network in the international scope. To this end, initiatives trying to find the widest possible dissemination will be launched in various international forums (European Commission, International Conference of Data Protection and Privacy Authorities, Organization of American States, etc.)

In short, the work carried out by the entities that make up the RIPD, which has finally led to the approval of the aforementioned Standards, constitutes a concrete experience of cooperation which, in our opinion, can be very useful for other organizations. Therefore, these standards are at the disposal of all entities and professionals who can benefit from them, in order to most effectively ensure the possible exercise and protection of the right to data protection in both the Ibero-American region as well as in an international context.

The Ibero-American States:

(1) Considering that the protection of individuals regarding treatment of their personal data is a fundamental right that is acknowledged at the highest level in most of the Constitutions of the Ibero-American States, under personal data protection law, or habeas data, and that in some cases it has been defined in court cases by its Courts or Constitutional Courts.

(2) Determining that the right to the protection of personal data has been conceptualized in some Ibero-American countries, by legal provisions and by court cases, as a right of a different nature than the right to private and family life, to intimacy, to honor, to a good name, and other similar rights that collectively guarantee the free development of an individual's personality, until it becomes an autonomous right, with its own characteristics and dynamics, which purpose is to safeguard the power of disposition and control that any individual has with regard to the information that concerns him, basically regarding the use of information and communication technology, which are increasingly relevant in every aspect of daily life.

(3) Assuming that safeguarding the right of the individuals with respect to the treatment of their personal data is compatible with the purpose of guaranteeing and protecting other rights, which are acknowledged as indivisible and interdependent among each other, and that require protection in order to safeguard individuals, in their wider scope, against illegal or arbitrary intrusions, and even those resulting from the treatment of personal data. The foregoing does not prevent applying the right to the protection of personal data to legal entities, in compliance with the provisions of the internal law of the Ibero-American States.

(4) Remembering that the Ibero-American Data Protection Network emerged in connection with the agreement reached in the Ibero-American Data Protection Conference, held in La Antigua, Guatemala, from June 1 to 6, 2003, with 14 Ibero-American countries in attendance. This initiative had, since the beginning, a political support reflected in the Final Declaration of the XIII Ibero-American Summit of Heads of State and Government, held in Santa Cruz de la Sierra, Bolivia, on November 14 and 15, 2003, aware of the nature of personal data protection as a fundamental right.

(5) Taking into consideration the on the occasion of the Resolution taken in the XXV Ibero-American Summit of Heads of State and Government, which was held in Cartagena de Indias, Colombia on October 28 and 29, 2016, it was reaffirmed that the adoption, preparation and promotion of different manuals, programs, initiatives and projects would strengthen the management and effect of cooperation actions among Ibero-American countries.

(6) Assuming that the Ibero-American Network is formed in a permanent forum for the exchange of information, open to all member countries of the Ibero-American Community, and that it allows the involvement of the public, private and social sectors, with the purpose of promoting the necessary regulatory developments in order to guarantee an advanced regulation of the right to the protection of personal data in a democratic and global context;

(7) Remembering that on the occasion of the meeting held in Santa Cruz de la Sierra, Bolivia, on May 3 to 5, 2006, the document called Guidelines for the Harmonization of Data Protection in the Ibero-American Community was prepared, which establishes a set of provisions which purpose is to contribute to the preparation of the regulatory initiatives for data protection that may arise in the Ibero-American Community, establishing themselves as a reference for the development of these Standards.

(8) Taking into consideration that the European Union has adopted a new regulatory framework on the matter, with the purpose of modernizing its provisions and guaranteeing greater soundness and consistency in the effective protection of the fundamental right to personal data protection in the European Union, and with the purpose of generating trust in society in general and, in turn, to facilitate the development of a digital economy, both in its internal market as in its global relations, this regulatory framework is positioned as a benchmark for the preparation of the national laws for data protection in Ibero-America.

(9) Acknowledging that there is a lack of harmonization in the Ibero-American States regarding the acknowledgment, adoption, definition and development of the figures, principles, rights and procedures that provide the contents of the right to personal data protection in their national laws, which without any doubt, is currently preventing these countries from facing the new challenges for the protection of this right, resulting from the ongoing and rapid technological evolution and globalization in various fields.

(10) Becoming a pressing fact within the framework of constant technological innovation, the adoption of regulatory instruments that guarantee, on the one hand, the protection of the individuals regarding the treatment of their personal data, that is currently the

base for the development, strengthening and exchange of goods and services in a global and digital economy, over which the economies of the Ibero-American states are built.

(11) Agreeing that in order to guarantee a high level of protection of the rights and freedoms of the individuals, we require in turn, among other matters, a uniform and high level of protection of the individuals regarding their personal information, which answers to current needs and demands in a global context, with the purpose of not raising barriers against free circulation of personal data in the Ibero-American States, and, therefore, favoring commercial activities in the region, as well as other economic regions.

(12) Accepting that with the purpose of widening and strengthening the regime of the protection of individuals regarding the treatment of their personal data, it is imperative to establish a balance among the interests of all the actors in the public, private and social sector and the holders involved, including the establishment of exceptions due to public interest matters that are reasonable and compatible with rights and freedoms, in order to prevent incurring in unjustified or disproportionate restrictions or limitations, that are not consistent with the purposes of democratic societies.

(13) Being aware of the potential risks that could result within the sphere of the individuals, due to the treatment of their personal data on a large scale, by public and private bodies, and specifically, taking into consideration the particular vulnerability of girls, boys and adolescents, who demand appropriate and sufficient protection guarantees, preserving in this way their best interest, the free development of their personality, their safety and other values that are subject to the highest protection by the Ibero-American States.

(14) Agreeing that technological development facilitates the treatment of new categories of personal data that represent specific risks, specially the inappropriate use thereof; therefore, it is highly relevant to achieve a minimum consensus regarding the categories of personal data considered sensitive or especially protected, as well as the rules for their treatment, taking into consideration that the consequences and negative interference that could result from the inappropriate use of these type of personal data can generate unfair or discriminatory conditions for individuals.

(15) Admitting that not all the Ibero-American States have laws on the matter, a situation that can affect the safeguarding and treatment of personal information, if we take into consideration the accelerated use of information technology that facilitates and allows massive communication of personal data in an immediate and almost unlimited way;

(16) Establishing that the laws on protection of personal data in the Ibero-American States must adopt the references contained in these Standards, in order to have a harmonized regulatory framework that offers a level of protection to individuals, regarding the treatment of their personal data and, in turn, guaranteeing the commercial and economic development of the zone;

(17) Admitting that currently the legal bases that legitimize every public or private body in order to treat the personal data in their possession are holder's consent; compliance with a legal provision; compliance with a court order, a founded and motivated resolution or mandate from a competent public authority; the exercise of the powers of public authorities; the acknowledgment or defense of holder's rights before a competent public authority; the execution of an agreement or pre-agreement in which holder is a part; compliance with a legal obligation applicable to the person responsible; the protection of holder's or another individual's vital interests; the legitimate interest of the public or private body; or due to reasons of public interest;

(18) Emphasizing the need to treat personal data under the same standards and homogeneous rules offered to holders of the same protection guarantees in the Ibero-American States, by establishing a mandatory catalog of principles, that responds to the current national and international standards on the matter, as well as the demands of an effective exercise and respect of this fundamental right.

(19) Acknowledging that with the purpose of effectively guaranteeing the right to the protection of personal data, it is necessary to adopt a regulatory framework that acknowledges any individual, in his capacity as holder of his personal data, the possibility of exercising, by general rule, in a without any charge, and exceptionally with an additional cost, due to reproduction, shipping, certification or others, the rights of access, correction, cancellation, opposition and portability, even in the context of the treatment of personal data performed by search engines in the Internet; these rights supplement the necessary conditions for holders to fully exercise their right to information self-determination.

(20) Highlighting the importance and fundamental role that service providers that treat personal data in the name and on behalf of the person responsible, including those that provide computer services in the cloud and other matters, which leads the Ibero-American States to adopt, in a global world, a regime that allows them to regulate this type of services, with the purpose of establishing a series of guarantees for the protection of the personal data, that they have and treat due to their commission, without releasing the person responsible from its duties and responsibilities before holders and control authorities.

(21) Considering that the development of new information and communication technologies, as well as the services developed within the context of a digital economy, are contributing to the continuous growth of the trans-border flow of personal data within the framework of a global society, the obligation to establish a minimum base that facilitates and allows those responsible and those in charge, in their capacity as exporters, the performance of international transfers of personal data, fully respecting holders' rights, is unavoidable.

(22) Taking into consideration that it is possible, through the Internet, to access and collect information available in any country, as well as to treat it, such as collecting information from millions of people without being physically established there, a circumstance that should not be a factor that prevents the effective protection of the rights and freedoms of individuals in the cyberspace.

(23) Acknowledging the importance of adopting preventive measures that allow the person responsible to proactively respond to the possible problems related to the adoption of binding self-regulation schemes or certification systems on the matter; appointing a personal data protection officer; preparing impact assessments on the protection of personal data and privacy by default and by design, among others, which is essential within the field of information and communication technology.

(24) Admitting the compelling need for each Ibero-American State to have an independent and impartial control authority, which decisions can only be appealed by judicial control, free of any external influence, with supervision and investigation powers on personal data protection, and in charge of supervising compliance with national legislation on the matter, which must be granted sufficient human and material resources in order to guarantee the exercise of its powers and the effective performance of its functions;

(25) Acknowledging that the Ibero-American States are bound to adopt a regime that guarantees holders a series of mechanisms and procedures in order to submit their claims before the control authority, when they consider that their right to the protection of personal data has been violated, as well as to be compensated when they have suffered damages and lost profits as a consequence of the violation of their right;

(26) Emphasizing the importance of establishing a minimum base for international cooperation between the Latin American control authorities, and between them and those of third party countries, with the purpose of encouraging and facilitating the application of the legislation on the matter, and an effective protection of the holders.

They have agreed to adopt these Standards as a maximum priority in the Ibero-American Community in order for them to contribute, in the capacity as orienting guidelines, to the issuance of regulatory initiatives for the protection of personal data in the region of the countries that do not have these laws yet, or if applicable, to serve as reference for the modernization and update of the existing legislations, encouraging the adoption of a harmonized regulatory framework that offers an appropriate level of protection to the individuals, regarding the treatment of their personal data and guaranteeing, in turn, the commercial and economic development of the regions, under the following:

Chapter I

General Provisions

1. Purpose

1.1 The purpose of these Standards is to:

a. Establish a set of principles and rights for the protection of personal data, which the Ibero-American States can adopt and develop in their national legislation, with the purpose of guaranteeing an appropriate treatment of personal data and having homogeneous rules in the region.

b. Raise the protection level of individuals, regarding the treatment of their personal data, as well as among the Ibero-American States, which answers to the international needs and demands that the right to the protection of personal data demands in a society in which information and knowledge technology are increasingly relevant in all matters of daily life.

c. Guarantee the effective exercise and safeguarding of the right to the protection of personal data of any individual in the Ibero-American States, by establishing common rules that ensure due treatment of their personal data.

d. Facilitate the flow of personal data among the Ibero-American States and beyond their borders, with the purpose of helping the social and economic growth of the region.

e. Drive the development of mechanisms for the international cooperation among the control authorities of the Ibero-American States, the control authorities that do not belong to the region, and international authorities and entities on the matter.

2. Definitions

2.1. For the purposes of these Standards it shall be understood as:

a. **Anonymization:** the application of measures of any kind aimed at preventing the identification or re-identification of an individual without disproportionate efforts.

b. **Consent:** expression of the free, specific, unequivocal and informed will of holder through which he accepts and authorizes the treatment of the personal data that concern him.

c. **Personal Data:** any information regarding an individual identified or identifiable, expressed in a numerical, alphabetical, graphical, photographic, alpha-numeric, acoustic way, or of any other kind. It is considered that a person is identifiable when his identity can be determined directly or indirectly, provided that this does not require disproportionate deadlines or activities.

d. **Sensitive Personal Data:** those that refer to the intimate sphere of their holder, or which undue use may originate discrimination or involve a serious risk thereto. In an illustrative way, personal data that may reveal aspects such as racial or ethnic origin; beliefs or religious, philosophical and moral convictions; union affiliation; political opinions; information regarding health, life, sexual preference or orientations, generic data or biometric data aimed at identifying the person in an unequivocal way.

e. **Person in Charge:** Service provider, which in its capacity as individual, or legal entity, or public authority, outside the organization of the responsible person, treats personal data in the name and on behalf thereof.

f. **Exporter:** individual or private legal entity, public authority, services, body, or service provider, located in the territory of a State that makes international transfer of personal data, according to the provisions of these Standards.

g. **Person Responsible:** individual or private legal entity, public authority, services or body that, alone or together with others, determines the purposes, means, scope and other matters related to the treatment of personal data.

h. **Holder:** individual to whom the personal data concern.

i. **Treatment:** any operation or set of operations performed through physical or automated procedures on personal data, related to, but not limited to, the collection, access, registration, organization, structuring, adaptation, indexation, modification, extraction, consultation, storage, preservation, development, transfer, dissemination, possession, exploitation, and in general, any use or disposal of personal data.

3. Subjective Field of Application

3.1. These Standards shall apply to individuals or private legal entities, authorities and public bodies that treat personal data in the course of their activities and functions.

4. Objective Field of Application

4.1. These Standards shall apply to the treatment of personal data contained in physical, fully or partially or both, automated media, regardless of the form or modality of their creation, type of media, processing, storage and organization.

4.2. As a general rule, these Standards shall apply to the personal data of individuals, which does not prevent the Ibero-America States to state in their legislation that the information of legal entities must be safeguarded in accordance with the right to the protection of personal data, in compliance with its internal law.

4.3. These Standards shall not apply under the following assumptions:

a. When personal data is intended for activities exclusively within the family life or domestic framework of an individual, i.e. the use of personal data within a friendship or kinship environment, or a close personal group, and that it is not intended for disclosure or commercial use.

b. Anonymous information, this means information that is not related to an identified or identifiable individual, as well as personal data subject to an anonymization process, in such way that holder cannot be identified or re-identified.

4.4. National legislation of the Ibero-American States applicable to the matter may establish categories of personal data, to which the protection regime provided in these Standards does not apply, in compliance with their internal law.

5. Field of Territorial Application

5.1. The Standards shall apply to the treatment of personal data performed:

a. By a person responsible or in charge, established in the territory of the Ibero-American States.

b. By a person responsible or in charge, not established in the territory of the Ibero-American States, when treatment activities are related to the offer of goods or services aimed at residents of the Ibero-American States, or to the control of their behavior, to the extent in which it happens within the Ibero-American States.

c. By a person responsible or in charge, not established in the territory of an Ibero-American State, but to whom the national legislation of such States applies, as the result of the execution of an agreement or under public international law.

d. By a person responsible or in charge, not established in the territory of the Ibero-American States that uses means, whether automated or not, located in such territory, in order to treat personal data, unless such means are only used with transit purposes.

5.2. For the purposes of these Standards, it shall be understood as establishment, the site of the central or main administration of the person responsible or in charge, which shall be determined based on objective criteria, and shall imply the effective and real exercise of management activities that determine the main decisions regarding the purposes and means of the treatment of personal data that they perform, through stable modalities.

5.3. The presence and use of technical and technological means for treating personal data, or for the treatment activities, shall not constitute, in themselves, a main establishment and shall not be considered as decisive criteria for defining the main establishment of the person responsible or in charge.

5.4. When personal data treatment is performed by a corporate group, the main establishment of the company that exercises control must be considered as the main establishment of the corporate group, except when the purposes and means of the treatment are effectively determined by another company in the group.

6. General Exceptions to the Right to the Protection of Personal Data

6.1. National legislation of the Ibero-American States, applicable to the matter, may limit the right to the protection of data in order to safeguard national security, public security, public health protection, the protection of rights and freedoms of third parties, as well as due to public interest matters.

6.2. Limitations and restrictions shall be expressly acknowledged in the law, with the purpose of providing sufficient certainty to holders, regarding the nature and scope of the measure.

6.3. Any law which purpose is to limit the right to the protection of personal data shall contain, at least, provisions regarding:

a. The purpose of the treatment.

b. The categories of the personal data in question.

c. The scope of the established limitations.

d. The appropriate guarantees for preventing illegal or disproportionate access or transfer.

e. Determining the person or persons responsible.

f. The deadlines for storing personal data.

g. The possible risks to holders' rights and freedoms.

h. Holders' rights to be informed about this limitation, unless it is harmful or incompatible with the purposes thereof.

6.4. The laws shall be the necessary, appropriate and proportionate ones in a democratic society, and must respect holders' fundamental rights and freedoms.

7. Deliberation on the Right to the Protection of Personal Data

7.1. Ibero-American States may exempt, in their internal law, compliance with the principles and rights provided in these Standards, only to the extent in which it is necessary to conciliate the right to the protection of personal data with other fundamental rights and freedoms.

7.2. This exemption shall require a deliberation exercise with the purpose of determining the need, suitability and proportionality of the restriction or exception according to the rules and criteria established by the Ibero-American States in their internal law.

8. Treatment of Personal Data of Girls, Boys and Adolescents

8.1. The Ibero-American States shall privilege the protection of the best interest of girls, boys and adolescents, in the treatment of the personal data thereof, in accordance with the Convention on the Rights of the Child and other international instruments that seek their well-being and comprehensive protection.

8.2. Ibero-American States shall promote in the academic education of girls, boys and adolescents, the responsible, appropriate and safe use of information and communication technology, and the eventual risks they face in digital environments regarding undue treatment of their personal data, as well as the respect of their rights and freedoms.

9. Treatment of Sensitive Personal Data

9.1. As a general rule, the person responsible may not treat sensitive personal data, except under the following assumptions:

a. That they are strictly necessary for the exercise and compliance with the powers and obligations expressly provided in the rules that regulate their actions.

b. They comply with a legal mandate.

c. They have holder's express written consent.

d. They are necessary for national security, public security, public order, public health reasons, or for the safekeeping of the rights and freedoms of third parties.

9.2. National legislation of the Ibero-American States applicable to the matter may establish exceptions, additional guarantees and conditions, in order to ensure due treatment of sensitive personal data, in accordance with its internal law.

Chapter II

Protection of Principles on Personal Data

10. Principles Applicable to the Treatment of Personal Data

10.1. When treating personal data, the person responsible shall observe the principles of legitimation, legality, loyalty, transparency, purpose, proportionality, quality, responsibility, safety and confidentiality.

11. Legitimation Principle

11.1. As a general rule, the person responsible may only treat personal data, under the following assumptions:

a. Holder grants its consent for one or several specific purposes.

b. Treatment is necessary for compliance with a court order, resolution or mandate, based and motivated by a competent public authority.

c. Treatment is necessary for exercising the powers belonging to public authorities, or are performed under legal power.

d. Treatment is necessary for the acknowledgment or defense of holder's rights before a public authority.

e. Treatment is necessary for the execution of an agreement or pre-agreement to which holder is part.

f. Treatment is necessary for compliance with a legal obligation applicable to the person responsible.

g. Treatment is necessary for protecting holder's or another individual's vital interests.

h. Treatment is necessary for public interest reasons established or provided by law.

i. Treatment is necessary for satisfying the legitimate interests of the person responsible or of a third party, as long as holder's interests or fundamental rights and freedoms that require the protection of personal data do not prevail over such interests, especially when holder is a boy, girl or adolescent. The above shall not apply to the treatment of personal data performed by public authorities when exercising their functions.

11.2. In the case of the last item, the treatment of personal contact data that is indispensable for locating individuals who provide their services to the person responsible shall be unders-

tood as covered by the legitimate interest, with the purpose of maintaining any type of relation with the person responsible.

12. Conditions for Consent

12.1. When it is necessary to obtain holder's consent, the person responsible shall prove in an indubitable way that holder granted its consent, whether through a clear representation or affirmation.

12.2. Whenever consent is required for the treatment of personal data, holder may revoke it at any time, for which the person responsible shall establish simple, agile, efficient and free mechanisms.

13. Consent for the Treatment of Personal Data of Girls, Goys and Adolescents

13.1. When obtaining the consent of girls, boys and adolescents, the person responsible shall obtain the consent of the holder of the parental rights or the tutor, in accordance with the provisions of the rules of representations provided in the internal law of the Ibero-American States, or if applicable, it shall directly request the authorization of the minor, if the internal law of each Ibero-American State has established a minimum age when he can grant it directly and without any representation from the holder of the parental rights or the tutor.

13.2. The person responsible shall make reasonable efforts to verify that the consent was granted by the holder of the parental rights or the tutor, or directly by a minor, according to his age, in accordance with the internal law of each Ibero-American State, taking into consideration the available technology.

14. Lawfulness Principle

14.1. The person responsible shall treat the personal data in its possession with strict adherence to and compliance with the applicable provisions of the internal law of the Ibero-American State, international law and the rights and freedoms of the individuals.

14.2. Treatment of personal data performed by public authorities shall be subject to the powers expressly granted to them by the internal law of the Ibero-American State in question, in addition to the provisions of the previous item of these Standards.

15. Loyalty Principle

15.1. The person responsible shall treat the personal data in its possession privileging the protection of holder's best interest and refraining from treating them through deceiving or fraudulent means.

15.2. For the purposes of these Standards, those treatments of personal data that result in unfair or arbitrary discrimination against holders shall be considered unfair.

16. Transparency Principle

16.1. The person responsible shall inform holder about the existence and main characteristics of the treatment to which its personal data shall be submitted, in order to make informed decisions on this regard.

16.2. The person responsible shall provide holder, at least the following information:

a. Its identity and contact information.

b. The purposes of the treatment to which its personal data shall be submitted.

c. The communications, whether national or international, of personal data that it intends to perform, including the recipients and the purposes that give rise to the performance thereof.

d. The existence, form and mechanisms or procedures through which it may exercise the access, correction, cancellation, opposition and portability rights.

e. If applicable, the origin of the personal data when the person responsible did not obtain them directly from holder.

16.3. The information provided to holder must be sufficient and easily accessible, as well as written and structured in a clear and simple language, easy for holders to whom it is addressed to understand, especially in the case of girls, boys and adolescents.

16.4. Every person responsible shall have transparent policies for the treatment of the personal data that it performs.

17. Purpose Principle

17.1. Every treatment of personal data shall be limited to compliance with defined, explicit and legitimate purposes.

17.2. The person responsible may not treat the personal data in its possession for purposes other than those that gave rise to the original treatment thereof, unless any of the causes that enable a new treatment of data according to the legitimation principle occurs.

17.3. Further treatment of personal data with filing, scientific or historic research, or statistical purposes, all of them in favor of public interest, shall not be considered incompatible with the initial purposes.

18. Proportionality Principle

18.1 The person responsible shall only treat the personal data that is appropriate, pertinent and limited to the minimum necessary regarding the purposes that justify their treatment.

19. Quality Principle

19.1. The person responsible shall adopt the necessary measures in order to keep the personal data in its possession accurate, complete and updated, in such way that the veracity thereof is not altered, as required for compliance with the purposes that gave rise to its treatment.

19.2. When personal data has stopped being necessary for compliance with the purposes that originated its treatment, the person responsible shall delete or remove it from its archives, records, data bases, files, or information systems, or if applicable, shall submit it to an anonymization procedure.

19.3. When removing personal data, the person responsible shall implement methods and techniques aimed at the final and safe removal thereof.

19.4. Personal data shall only be kept during the necessary term for complying with the purposes that justify its treatment or those related to legal demands applicable to the person responsible. However, national legislation of the Ibero-American States, applicable to the matter, may establish exceptions regarding the term of preservation of personal data, with full respect to holder's rights and guarantees.

20. Responsibility Principle

20.1. The person responsible shall implement the necessary mechanisms to prove compliance with the principles and obligations established in these Standards, and shall also be accountable to holder and to the control authority for the treatment of personal data in its possession, for which it may use standards, best national or international practices, self-regulation schemes, certification systems, or any other mechanism it deems appropriate for such purposes.

20.2. The foregoing shall apply when personal data is treated by a person in charge in the name and on behalf of the person responsible, as well as at the time of making transfers of personal data.

20.3. Among the mechanisms that the person responsible may adopt to comply with the responsibility principle are, without limitation, the following:

a. Allocate resources for the implementation of programs and policies for the protection of personal data.

b. Implement risk management systems related to the treatment of personal data.

c. Prepare mandatory and enforceable personal data protection policies and programs, within the organization of the person responsible.

d. Implement a training and updating program for personnel about obligations on personal data protection matters.

e. Periodically review the personal data safety policies and programs, in order to determine the required modifications.

f. Establish an internal and/or external supervision and surveillance system, including audits, in order to prove compliance with the policies for the protection of personal data.

g. Establish procedures for receiving and answering questions and complaints from holders.

20.4. The person responsible shall permanently review and assess the mechanisms that it voluntarily adopts in order to comply with the responsibility principle, with the purpose of assessing its efficiency level regarding compliance with applicable national legislation.

21. Safety Principle

21.1. The person responsible shall establish and maintain, regardless of the type of treatment it performs, sufficient administrative, physical and technical measures in order to guarantee the confidentiality, integrity and availability of personal data.

21.2. In order to determine the measures mentioned in the previous item, the person responsible shall take into consideration the following factors:

a. The risk to holders' rights and freedoms, especially, due to the quantitative and qualitative potential value that the treated personal data could have for a third party not authorized to have them.

b. The status of the technique.

c. The costs of the application.

d. The nature of the treated personal data, especially in the case of sensitive personal data.

e. The scope, context and purposes of the treatment.

f. International transfers of personal data that are done or intended to be done.

g. The number of holders.

h. The possible consequences that could result from a violation to holders.

i. Prior violations to the treatment of personal data.

21.3. The person responsible shall perform a series of actions that guarantee the establishment, implementation, operation, monitoring, revision, maintenance and continuous improvement of the security measures applicable to the treatment of personal data, in a periodical way.

22. Notice of Violation to the Safety of Personal Data

22.1. When the person responsible becomes aware that a violation to the safety of personal data has occurred in any phase of the treatment, understood as any damage, loss, alteration, destruction, access and, in general, any illegal or non-authorized use of personal data, even if it occurs accidentally, it shall notify the control authority and the affected holders of such event, without delay.

22.2. The foregoing shall not apply when the person responsible can prove, addressing the proactive responsibility principle, the improbability of the safety violation that occurred, or that it does not represent a risk to the rights and freedoms of the holders involved.

22.3. The notice made by the responsible person to the affected holders shall be drafted in clear and simple language.

22.4. The notice referred to in the previous numbers shall contain, at least, the following information:

a. The nature of the incident.

b. The compromised personal data.

c. Corrective actions taken immediately.

d. Recommendations to holder about the measures it may adopt to protect its interests.

e. The means available to holder for obtaining more information in this regard.

22.5. The person responsible shall document all safety violations of the personal data that happened at any time of the treatment, identifying, without limitation, the date when it happened, the reason for the violation; the facts related to it and their effects, and the corrective measures implemented in an immediate and definite way, which shall be available to the control authority.

22.6. National legislation of the Ibero-American States, applicable to the matter shall establish the effects of the notices of safety violations given by the person responsible to the control authority, regarding the procedures, form and conditions of its intervention, with the purpose of safeguarding the interests, rights and freedoms of the affected holders.

23. Confidentiality Principle

23.1. The person responsible shall establish controls or mechanisms in order for those who participate in any phase of the treatment of personal data to maintain and respect the confidentiality thereof, this obligation shall survive even after ending its relations with holder.

Chapter III

Holder's Rights

24. ARCO Rights

24.1. At all times holder or its representative may request from the person responsible access, correction, cancellation, opposition and portability of the personal data that concern it.

24.2. The exercise of any of the rights mentioned in the item above, is not a prior requirement, nor does it prevent exercising another right.

25. Right to Access

25.1. Holder shall have the right to request access to its personal data in possession of the responsible person, as well as to know any information related to the general and specific conditions of their treatment.

26. Right to Correction

26.1. Holder shall have the right to obtain from the person responsible the correction of its personal data when they are inaccurate, incomplete or are not updated.

27. Right to Cancellation

27.1. Holder shall have the right to request the cancellation or removal of its personal data from the archives, records, files and systems of the person responsible, in order for them not to be in its possession and for the person responsible to stop treating them.

28. Right to Opposition

28.1. Holder may oppose to the treatment of its personal data when:

a. It has a legitimate reason resulting from its particular situation.

b. The purpose of the treatment of its personal data is direct marketing, including preparing profiles, to the extent that it is related to such activity.

28.2 In the case of the previous item, when holder opposes treatment with direct marketing purposes, its personal data must stop being treated with such purposes.

29. Right not to be Subject to Automated Individual Decisions

29.1. Holder shall have the right not to be the subject of decisions that cause it legal effects, or that affect it in a significant way, based only on automated treatments intended to assess, without human intervention, some of his own personal aspects, or to analyze and predict, specifically, its professional performance, economic situation, health status, sexual preferences, reliability or behavior.

29.2. What the previous item provides shall not apply when the automated treatment of personal data is necessary for the execution of an agreement between holder and the person responsible; when it is authorized by the internal law of the Ibero-American States, or when it is based on provable consent from holder.

29.3. Nevertheless, when it is necessary for the contractual relation, or when holder has expressed its consent, it shall have the right to obtain human intervention; receive an explanation about the decision taken; express its point of view and appeal the decision.

29.4. The person responsible may not perform automated treatments of personal data in its possession which purpose is holders' discrimination due to their racial or ethnic origin; beliefs or religious, philosophical and moral convictions, union affiliation, political opinions; data related to health, life, sexual preference or orientation, as well as genetic or biometric data.

30. Right to Portability of Personal Data

30.1. In the case of personal data by telephone or automated means, holder shall have the right to obtain a copy of the personal data that it had provided to the person responsible, or that are subject to treatment, in a structured electronic format, of common use and mechanical reading, that allows it to keep using them and transfer them to another person responsible, in case it requires so.

30.2. Holder may request that its personal data are transferred directly from person responsible to person responsible when technically possible.

30.3. The right to portability of personal data shall not affect negatively the rights and freedoms of others.

30.4. Without prejudice to holder's rights, the right to portability of personal data shall not be admissible in the case of inferred, derived, created or generated information, or information obtained from the analysis or treatment performed by the person responsible, based on the personal data provided by holder, such as personal data that had been subject to a personalization, recommendation, categorization or profile creation process.

31. Right to the Limitation of Treatment of Personal Data

31.1. Holder shall have the right to have the treatment of its personal data limited to its storage during the period of time between a rectification or opposition request, until its resolution by the person responsible.

31.2. Holder shall have the right to limit the treatment of its personal data when it is not necessary for the person responsible, but it needs it in order to file a claim.

32. Exercise of the ARCO and Portability Rights

32.1. The person responsible shall establish simple, expeditious, accessible and free procedures that allow holder to exercise its rights to access, correction, cancellation, opposition and portability.

32.2. The national legislation of the Ibero-American States applicable to the matter, shall establish the requirements, deadlines, terms and conditions under which holders may exercise their access, correction, cancellation, opposition and portability rights, as well as the causes for inadmissibility to the exercise thereof, such as the following, without limitation:

a. When treatment is necessary for compliance with an important purpose of public interest.

b. When treatment is necessary for exercising the functions of public authorities.

c. When the person responsible proves having legitimate motives in order for the treatment to prevail over holder's interests, rights and freedoms.

d. When treatment is necessary for compliance with a legal provision.

e. When personal data is necessary for maintenance and compliance with a legal or contractual relation.

32.3. The national legislation of the Ibero-American States applicable to the matter may acknowledge that individuals related to deceased individuals or appointed by them, exercise the rights referred to in this standard, regarding the personal data of the deceased person of their concern.

32.4. The national legislation of the Ibero-American States applicable to the matter shall acknowledge holder's right to oppose or appeal the answers granted by the person responsible in the case of a request to exercise the rights mentioned in this item, or in case of lack of response from it, before the control authority, and if applicable, before judicial authorities in accordance with the internal right of each Ibero-American State.

Chapter IV

Person in Charge

33. Scope of the Person in Charge

33.1. The person in charge shall perform the treatment activities of the personal data without having any decision power over the scope and contents thereof, and it shall limit its acts to the terms established by the person responsible.

34. Formalization of the Provision of Services of the Person in Charge

34.1. The provision of services between the person responsible and the person in charge shall be formalized by executing an agreement, or any other legal instrument, considered by the Ibero-American States in the national legislation applicable to the matter.

34.2. The agreement or legal instrument shall establish, at least, the subject, scope, contents, duration, nature and purpose of the treatment, type of personal data; holders' categories, as well as the obligations and responsibilities of the person responsible and the person in charge.

34.3. The agreement or legal instrument shall establish at least, the following general clauses related to the services provided by the person in charge:

a. Treat the personal data according to the instructions of the person responsible.

b. Refrain from treating the personal data with purposes other than those instructed by the person responsible.

c. Implement the safety measures in accordance with applicable legal instruments.

d. Inform the person responsible when a violation occurs to the personal data that it is treating per the instructions of the person responsible.

e. Maintain the confidentiality regarding the treated personal data.

f. Suppress, return or communicate to a new person in charge, appointed by the person responsible, the personal data subject to treatment, once the legal relation with the person responsible has been met, or per its instructions, except if a legal provision demands keeping the personal data, or the person responsible authorizes communicating them to another person in charge.

g. Refrain from transferring the personal data, except in case that the person responsible determines so, or that the communication results from a sub-contract, or by express mandate from the control authority.

h. Allow the person responsible or the control authority to make in situ inspections and verifications.

i. Generate, update and keep the necessary documentation that allows it to prove its obligations.

j. Cooperate with the person responsible in everything related to compliance with the national legislation of the Ibero-American State that is applicable to the matter.

34.4. When the person in charge fails to comply with the instructions from the person responsible, and decides itself on the scope, contents, means and other matters of the treatment of personal data, it shall assume the responsibility according to the national legislation of the Ibero-American State that applies to the matter.

35. Subcontracting Services

35.1. The person in charge may, in turn, sub-contract services that imply the treatment of personal data, provided that there is a prior written, specific or general, authorization from the person responsible, or it is expressly stipulated in the agreement or legal instrument executed by the latter and the person in charge.

35.2. Subcontractor shall assume the capacity as person in charge under the terms stated in the national legislation of the Ibero-American State applicable to the matter.

35.3. The person in charge shall formalize the provision of subcontractor's services through an agreement or any other legal instrument determined by the national legislation of the Ibero-American State, that applies to the matter.

35.4. When subcontractor fails to comply with its obligations and responsibilities regarding the treatment of personal data it performs according to what the persons in charge instructed, it shall be responsible according to the national legislation of the Ibero-American State applicable to the matter.

Chapter V

International Transfers of Personal Data

36. General Rules for Transferring Personal Data

36.1. The person responsible and the person in charge may perform international transfers of personal data under any of the following assumptions:

a. The country, part of its territory, sector, activity or international organization, recipient of the personal data has been acknowledged as having an appropriate level of protection of personal data by the transferring country, in accordance with the national legislation of the latter, which applies to the matter, or the recipient country, or several sectors thereof, prove minimum and sufficient conditions to guarantee an appropriate level of protection of personal data.

b. Exporter offers sufficient guarantees for the treatment of personal data in the recipient country, and the latter, in turn, proves compliance with the minimum and sufficient conditions established in the national legislation, applicable to the matter, of each of the Ibero-American States.

c. Exporter and recipient sign contractual clauses or any other legal instrument that offers sufficient guarantees and that allows proving the scope of the treatment of the personal data, the obligations and responsibilities assumed by the parties, and holders' rights. The control authority may validate the contractual clauses or legal instruments, as determined in the national legislation on the matter, of the Ibero-American States.

d. Exporter and recipient adopt a binding self-regulation scheme or an approved certification mechanism, provided that it is consistent with the provisions of the national legislation of the Ibero-American State applicable to the matter, which exporter is bound to observe.

e. The control authority of the Ibero-American State of exporter authorizes the transfer, under the terms of the national legislation applicable to the matter.

36.2. National legislation of the Ibero-American States, applicable to the matter, may expressly establish limits to international transfers of categories of personal data, for reasons of national security, public security, public health protection, the protection of rights and freedoms of third parties, as well as due to public interest matters.

Chapter VI

Proactive Measures in the Treatment of Personal Data

37. Acknowledgment of Proactive Measures

37.1. The national legislation of the Ibero-American States applicable to the matter may acknowledge and establish measures that promote better compliance with their legislation, and that help strengthening and increasing protection controls of personal data implemented by the person responsible, among which the ones stated in this Chapter may be found.

38. Privacy Due to Design and Privacy by Default

38.1. The person responsible shall apply, from the design, in the determination of the treatment means of personal data, during and before the collection of personal data, preventive measures of various natures that allow effectively applying the principles, rights and other obligations provided in the applicable national legislation of the Ibero-American State.

38.2. The person responsible shall guarantee that its programs, services, computing systems or platforms, electronic applications or any other technology that implies a treatment of personal data, comply by default or adapt to the principles, rights and other obligations provided in the applicable national legislation of the Ibero-American State. Specifically, with the purpose that only a minimum of personal data is subject to treatment, and that the accessibility thereof is limited, without holder's intervention, to an undetermined number of persons.

39. Official Protection of Personal Data

39.1. The person responsible shall appoint a personal data protection officer or an equivalent figure in those cases established in the applicable national legislation of the Ibero-American States, and when:

a. It is a public authority.

b. It performs treatments of personal data which purpose is the regular and systematic observation of holder's conduct.

c. Performs treatments of personal data where it is probable that it entails a high risk of affecting the right to the protection of holders' personal data, taking into consideration, among other factors and without limitation, the categories of the personal data treated, especially in the case of sensitive data; the transfers made; the number of holders; the scope of the treatment; the information technology used or their purposes.

39.2. The person responsible that is not under any of the circumstances provided in the item above, may appoint a personal data protection officer, if it deems it convenient.

39.3. The person responsible shall be bound to back-up the personal data protection officer in the performance of his functions, facilitating the necessary resources for his performance and for maintaining his specialized knowledge and the update thereof.

39.4. The personal data protection officer shall have at least the following functions:

a. Advise the person responsible regarding the topics that are submitted for his consideration on the matter or personal data protection.

b. Coordinate, inside the organization of the person responsible, the policies, programs, actions and other activities that correspond to compliance with the applicable national legislation of the Ibero-American State.

c. Supervise inside the organization of the person responsible compliance with the applicable national legislation of the Ibero-American State.

40. Self-regulation Mechanisms

40.1. The person responsible may voluntarily adhere to the binding self-regulation scheme, which purpose is, among others, to contribute to the correct application of the applicable national legislation of the Ibero-American State, and to establish procedures for resolving conflicts between the person responsible and holder, without prejudice to other mechanisms established in the national legislation of the applicable matter, taking into consideration the specific characteristics of the treatments of personal data performed, as well as the effective exercise of and respect to holder's rights.

40.2. For the purposes of the previous item, codes of ethics and certification systems can be developed, among others, with their respective trust marks that contribute to the purposes stated in this item.

40.3. National legislation of the Ibero-American code applicable to the matter shall establish the rules that correspond for the validation, confirmation or acknowledgment of the aforementioned self-regulation mechanisms.

41. Impact Assessment on the Protection of Personal Data

41.1. When the person responsible intends to perform a type of treatment of personal data that due to its nature, context or purposes probably entails a high risk of affecting the right to the protection of holders' personal data, it shall perform, prior to the implementation thereof, an impact assessment on the protection of personal data.

41.2. National legislation of the Ibero-American States that is applicable to the matter shall state the treatments that require an impact assessment on the protection of personal data; the contents thereof, the assumptions under which the result must be submitted to the control authority, as well as the requirements of said submission, among other matters.

Chapter VII

Control Authorities

42. Nature of Control and Supervision Authorities

42.1. There must be one or more control authorities on personal data protection in each Ibero-American State, with full autonomy, in accordance with their applicable national legislation.

42.2. Control authorities may be single-member or multiple-member bodies; they shall act impartially and independently in their jurisdictions, and they shall be free or any external influence, whether direct or indirect, and they shall not request nor admit any order or instruction.

42.3. The member or members of the direction bodies of the control authorities must have the necessary experience and skills, especially with respect to the field of personal data protection, for compliance with their functions and the exercise of their powers. They shall be appointed through a transparent procedure under applicable national legislation and may only be removed due to serious causes, established in the internal law of each Ibero-American State, according to the rules of due process.

42.4. The applicable national legislation of the Ibero-American States must grant the control authorities sufficient investigation, supervision, resolution, promotion, sanction and other powers that are necessary in order to guarantee effective compliance with it, as well as the exercise and respect of the right to the protection of personal data.

42.5. The decisions of the control authorities shall only be subject to jurisdictional control according to the mechanisms established in the national legislation of the Ibero-American States that is applicable to the matter and its internal law.

42.6. Control authorities must have the necessary human and material resources for complying with their functions.

Chapter VIII

Claims and Sanctions

43. Claim and Sanction Regime

43.1. Every holder shall have the right to submit its claim before the control authority, as well as to due process of law, in order to make its rights effective in accordance with the applicable national legislation of the Ibero-American State.

43.2. National legislation of the Ibero-American States applicable to the matter shall establish a regime that allows holder to submit a claim before the control authority when it considers that the treatment of its personal data violates the national regulations on the matter, as well as to request due process of law.

43.3. National legislation of the Ibero-American States applicable to the matter, shall establish a regime that allows the adoption of corrective measures, and to sanction conducts that contravene the provisions of the relevant national legislations, stating, at least, the maximum limit and the objective criteria for establishing the relevant sanctions, in accordance with the nature, severity and duration of the violation, and its consequences, as well as the measures implemented by the person responsible in order to guarantee compliance with its obligations on the matter.

Chapter IX

Right to Compensation

44. Restitution

44.1. National legislation of the Ibero-American States applicable to the matter shall acknowledge holder's right to be compensated when it has suffered damages and lost profits, a consequence of a violation to its right to the protection of personal data.

44.2. The internal law of the Ibero-American States shall state the competent authority that shall hear these types of actions filed by the affected holder, as well as the deadlines, requirements and terms through which it shall be compensated, in case it is admitted.

Chapter X

International Cooperation

45. Establishment of International Cooperation Mechanisms

45.1. The Ibero-American States may adopt international cooperation mechanisms that facilitate the application of applicable national legislations on the matter, which may include, without limitation:

a. Establishing mechanisms that allow reinforcing international assistance and cooperation in the application of the relevant national legislations on the matter.

b. The assistance between the control authorities through the notification and submission of claims, assistance in investigations, and information exchange.

c. The adoption of mechanisms aimed at the awareness and exchange of best practices and experiences on personal data protection matters, including jurisdiction conflicts with third party countries.