RED IBEROAMERICANA DE PROTECCION DE DATOS

Red Iberoamericana
Rede Ibero-Americana

Data Protection Standards of the Ibero-American States

Approved on 26 May 2026 in Cartagena de Indias, Colombia.



Background

As part of the 15th Ibero-American Data Protection Meeting, the Ibero-American Data Protection Network (RIPD or The Network) approved and officially presented the so-called 'Ibero-American Data Protection Standards', thereby fulfilling a long-standing objective shared by all the organisations that make up the Network, as well as one of the agreements adopted at the 25th Ibero-American Summit of Heads of State and Government, held in Colombia on 28 and 29 October 2016, which called on the Network to draw up a proposal for effective cooperation on the protection of personal data and privacy.

The approved text sought to address one of the strategic priorities agreed by the RIPD in November 2016 in Montevideo, as set out in the document "RIPD 2020". This priority consisted of "promoting and contributing to the strengthening and adaptation of regulatory processes in the region, through the development of guidelines that serve as a benchmark for future regulations or for the review of existing ones".

In this regard, the Ibero-American Standards constitute a set of guiding principles designed to assist in the development of regulatory initiatives for the protection of personal data in the Ibero-American region, both in those countries which do not yet have such legislation and, where appropriate, by serving as a benchmark for the modernisation and updating of existing legislation.

The following are among the **objectives** of the Ibero-American Standards:

- To establish a set of common personal data protection principles and rights which the Ibero-American States may adopt and incorporate into their national legislation, with a view to ensuring a consistent set of rules across the region.

- To ensure the effective exercise and safeguarding of the right to personal data protection for all natural persons in the Ibero-American States, by establishing common rules that guarantee the proper processing of their personal data

- To facilitate the flow of personal data between the Ibero-American States and beyond their borders, with the aim of contributing to the region's economic and social development.

- To promote international cooperation between the supervisory authorities of the Ibero-American States, supervisory authorities outside the region, and relevant international authorities and organisations.

As the immediate background to these Standards, mention may be made, on the one hand, of the adoption by the RIPD itself, in 2007, on the occasion of the 5th Ibero-American Data Protection Meeting, of the "Guidelines for the Harmonisation of Data Protection in the Ibero-American Community", which were intended to establish a "harmonised framework" as a reference for national regulatory initiatives arising in the region in the field of data protection; and, on the other hand, of the standards approved at the International Conference of Privacy and Data Protection Authorities, held in Madrid in 2009, the

so-called "Madrid Standards", which undoubtedly represented a step forward in the search for specific solutions and provisions "that could be applied regardless of any differences that might exist between the various existing models of data protection and privacy".

In drawing up the Ibero-American Standards, reference was also made to other key international instruments relating to the protection of personal data, such as the Organisation for Economic Co-operation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Protocol; the Asia-Pacific Economic Cooperation (APEC) Privacy Framework; and the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, amongst others.

With the adoption of these Standards, the RIPD gained an essential tool to rigorously monitor and support future legislative developments in the Region, as the Ibero-American Standards are characterised by being a regulatory model that:

- It responds to the national and international needs and requirements arising from the right to personal data protection, in a society where information and knowledge technologies are becoming increasingly important in every aspect of daily life.

- It includes national and international best practices in this field.

- It proposes a set of standards that are flexible enough to facilitate their adoption by Ibero-American States, without in any way contravening their domestic law, so that this document may become a living and viable reality in the Ibero-American region for the benefit of the data subject.

- It ensures an adequate level of protection for personal data in the Ibero-American region, with the aim of avoiding barriers to the free movement of such data within the Ibero-American States and, consequently, of promoting trade both within the region and with other economic regions.

The Ibero-American States:

(1) Whereas the protection of natural persons with regard to the processing of their personal data is a fundamental right recognised at the highest level in most of the Constitutions of the Ibero-American States, in the form of the right to the protection of personal data or *habeas data*, and that in some cases it has been defined in case law by their Constitutional Courts or Tribunals;

(2) Having established that the right to personal data protection has been conceptualised in some Ibero-American countries, either through legislation or case law, as a right distinct in nature from the rights to private and family life, privacy, honour, reputation and other similar rights, which together guarantee the free development of a natural person's personality, and that it has consequently become an autonomous right, with its own characteristics and dynamics, the purpose of which is to safeguard every natural person's power to dispose of and control

information concerning them, primarily in view of the use of information and communications technologies, which are becoming increasingly important in all aspects of daily life;

(3) On the assumption that safeguarding the right of natural persons with regard to the processing of their personal data is compatible with the objective of guaranteeing and protecting other rights, which are recognised as indivisible and interdependent, and which require appropriate protection to safeguard natural persons, in the broadest sense, against unlawful or arbitrary intrusions, including those arising from the processing of personal data.

(4) Recalling that the Ibero-American Data Protection Network arose from the agreement reached at the Ibero-American Data Protection Meeting, held in La Antigua, Guatemala, from 1 to 6 June 2003, and attended by representatives from 14 Ibero-American countries. This initiative enjoyed political support from the outset, as reflected in the Final Declaration of the 13th Summit of Heads of State and Government of the Ibero-American countries, held in Santa Cruz de la Sierra, Bolivia, on 14 and 15 November 2003, which acknowledged personal data protection as a fundamental right;

(5) Bearing in mind that, following the adoption of the Resolution at the 25th Ibero-American Summit of Heads of State and Government, which took place in Cartagena de Indias, Colombia, on 28 and 29 October 2016, it was reaffirmed that the adoption, development and promotion of various manuals, programmes, initiatives and projects would strengthen the management and impact of cooperation activities between the countries of Ibero-America;

(6) Assuming that the Ibero-American Data Protection Network constitutes a permanent forum for the exchange of information, open to all member countries of the Ibero-American Community, and that it facilitates the involvement of the public, private and social sectors, with the aim of promoting the necessary regulatory developments to ensure advanced regulation of the right to personal data protection within a democratic and global context;

(7) Recalling that, following the meeting held in Santa Cruz de la Sierra, Bolivia, from 3 to 5 May 2006, a document entitled 'Guidelines for the Harmonisation of Data Protection in the Ibero-American Community' was drawn up, which sets out a series of provisions intended to contribute to the development of regulatory initiatives on data protection arising within the Ibero-American Community, and serves as a benchmark for the development of the Standards;

(8) Bearing in mind that the European Union adopted a new regulatory framework in this area at the time, with the aim of modernising its provisions and ensuring greater robustness and consistency in the effective protection of the fundamental right to personal data protection, whilst also facilitating the development of the digital economy, both within its internal market and in its global relations; a regulatory framework which serves as an indispensable and decisive reference point for the drafting of national data protection legislation in Ibero-America;

(9) Recognising that there is a lack of harmonisation amongst the Ibero-American States with regard to the recognition, adoption, definition and development of the legal concepts, principles, rights and procedures that give substance to the right to personal data protection in their national legislation, which, undoubtedly, makes it difficult at present to address the new challenges to the protection of this right arising from constant and rapid technological evolution and globalisation in various fields;

(10) In the context of ongoing technological innovation, it is imperative to adopt regulatory instruments that guarantee, on the one hand, the protection of natural persons with regard to the

processing of their personal data and, on the other hand, the free flow of personal data, which currently forms the basis for the development, strengthening and exchange of goods and services in a global and digital economy, upon which the economies of the Ibero-American States are built; including effective mechanisms for the governance of processing, traceability and supervision of automated systems and artificial intelligence, aimed at ensuring the protection of fundamental rights and freedoms.

Taking into account, furthermore, the "Specific Guidelines for Compliance with the Principles and Rights Governing the Protection of Personal Data in Artificial Intelligence Projects" and the "General Recommendations on Data Processing in Artificial Intelligence" adopted by the Ibero-American Data Protection Network on 21 June 2019, in Naucalpan de Juárez, Mexico;

(11) Agreeing that, in order to ensure a high level of protection for the rights and freedoms of natural persons, among other things, a uniform and high level of protection for natural persons with regard to their personal data is also required, meeting current needs and requirements in a global context, with the aim of avoiding barriers to the free movement of personal data within the Ibero-American States and, consequently, promoting commercial activities both within the region and with other economic regions;

(12) Recognising that, with a view to expanding and strengthening the regime for the protection of natural persons with regard to the processing of their personal data, it is imperative to strike a balance between the interests of all actors in the public, private and social sectors and the data subjects concerned, including the establishment of exceptions on grounds of public interest that are reasonable and compatible with rights and freedoms, so as to avoid imposing unjustified or disproportionate restrictions or limitations that are inconsistent with the aims pursued in democratic societies;

(13) Recognising the potential risks that may arise for natural persons as a result of the large-scale processing of their personal data by public and private bodies and, in particular, taking into account the special vulnerability of children and adolescents, who require adequate and sufficient safeguards against the improper or arbitrary use of their personal information, thereby safeguarding their best interests, the free development of their personality, their safety and other values that are afforded the highest level of protection by the Ibero-American States. These risks may be exacerbated by automated processing, including processing carried out by artificial intelligence systems capable of inferring, classifying, profiling or significantly influencing individuals.

(14) Recognising that technological development facilitates the processing of new categories of personal data that present specific risks, in particular the inappropriate use of such data; it is therefore particularly important to reach a minimum consensus regarding the categories of personal data considered to be sensitive or subject to special protection, as well as the rules governing their processing, bearing in mind that the negative consequences and adverse effects that may arise from the misuse of this type of personal data may give rise to unfair or discriminatory conditions for natural persons;

(15) Whilst acknowledging that not all Ibero-American States have legislation in this area – a situation which may adversely affect the protection and processing of personal data – given the rapidly increasing use of information technologies that facilitate and enable the immediate and virtually unlimited mass communication of personal data;

(16) Stating that legislation on the protection of personal data in the Ibero-American States must adopt the benchmarks set out in these Standards in order to establish a harmonised regulatory framework that provides protection for natural persons with regard to the processing of their personal data and, in turn, guarantees the commercial and economic development of the region;

(17) Emphasising the need for personal data in the Ibero-American States to be processed in accordance with the same standards and uniform rules, thereby offering data subjects the same guarantees of protection, through the establishment of a catalogue of mandatory principles that reflects current national and international standards in this area, as well as the requirements for the effective exercise and respect of this fundamental right;

(18) Recognising that, in order to effectively guarantee the right to personal data protection, it is necessary to adopt a regulatory framework which recognises the right of any natural person, in their capacity as data subject, to exercise – as a general rule free of charge and, exceptionally, subject to costs associated with reproduction, dispatch, certification or other legitimate reasons – the rights of access, rectification, erasure, objection and data portability, including in the context of the processing of personal data carried out by internet search engines; rights which complement the conditions necessary for data subjects to fully exercise their right to informational self-determination;

(19) Emphasising the importance and fundamental role played by service providers who process personal data on behalf of and for the account of the controller, including those providing cloud computing services and other related services, which requires the Ibero-American States, in a globalised world, to adopt a framework enabling them to regulate such services with the aim of establishing a series of safeguards for the protection of personal data that they hold and process in the course of providing their services, without exempting the controller from its obligations and responsibilities towards data subjects and supervisory authorities;

(20) Whereas the development of new information and communications technologies, as well as the services developed within the context of the digital economy, are contributing to the continued growth of cross-border flows of personal data within a global society, it is essential to establish a minimum framework that facilitates and enables controllers and processors, in their capacity as exporters, to carry out international transfers of personal data whilst fully respecting the rights of data subjects;

(21) Bearing in mind that the Internet makes it possible to access and collect information available in any country, as well as to process such information – for example, by collecting data on millions of people without being physically established there – a circumstance which should not constitute a factor preventing the effective protection of natural persons' rights and freedoms in cyberspace;

(22) Recognising the importance of adopting preventive measures that enable the data controller to respond proactively to potential issues relating to the right to the protection of personal data, such as the adoption of binding self-regulatory schemes or certification schemes in this area; the appointment of a data protection officer; the carrying out of data protection impact assessments and the implementation of privacy by default and by design, amongst others, which are essential in the field of information technology and telecommunications; algorithmic governance, traceability, effective human oversight, continuous risk assessment, technical documentation and periodic auditing of automated systems and artificial intelligence.

(23) Recognising the urgent need for each Ibero-American State to have an independent and impartial supervisory authority, whose decisions may only be challenged through judicial review and which is free from any external influence, with powers of supervision and investigation in the field of personal data protection and responsible for monitoring compliance with national legislation in this area, and which has sufficient human and material resources to ensure that it can exercise its powers and perform its functions effectively;

(24) Recognising that the Ibero-American States are obliged to adopt a framework that guarantees data subjects a range of mechanisms and procedures for lodging complaints with the supervisory authority where they consider that their right to personal data protection has been infringed, as well as for obtaining compensation where they have suffered loss or damage as a result of a breach of that right;

(25) Emphasising the importance of establishing a minimum framework for international cooperation between Latin American supervisory authorities and between those authorities and supervisory authorities in third countries, with the aim of promoting and facilitating the application of the relevant legislation and the effective protection of data subjects;

They have agreed to adopt these Standards as a matter of the highest priority within the Ibero-American Community so that, in their capacity as guiding principles, they may contribute to the development of regulatory initiatives on personal data protection in those countries in the region which do not yet have such legislation, or, where appropriate, serve as a benchmark for the modernisation and updating of existing legislation, thereby promoting the adoption of a harmonised regulatory framework that provides an adequate level of protection for natural persons with regard to the processing of their personal data, whilst, at the same time, ensuring the region's commercial and economic development.

Chapter I. General Provisions

1. Purpose

1.1. The purpose of these Standards is:

a. To establish a set of regulatory parameters concerning the right to personal data protection, which will serve as guidance for legislators, public policy-makers and, more generally, decision-makers in the Ibero-American States in the drafting, design or modernisation of legislation, regulations and, more generally, any regulatory instruments in this area.

b. To contribute to promoting regulatory interoperability in the field of personal data protection, with the aim of fostering the development of regulatory frameworks that facilitate cooperation between personal data protection authorities and, in particular, the strengthening of the protection of fundamental rights and freedoms in Ibero-America, for the benefit of individuals.

c. To promote the effective exercise and protection of the right to personal data protection for any natural person in the Ibero-American States, through the development of common guidelines,

criteria and parameters that contribute to strengthening this right at national level, as well as across the Ibero-American region.

d. To establish common ground regarding international data transfers, in order to facilitate the flow of personal data between Ibero-American States and beyond their borders, with a view to contributing to the region's social development and economic growth.

e. To promote the development of mechanisms for international cooperation between the supervisory authorities of the Ibero-American States, supervisory authorities from outside the region, and international authorities and bodies in this field.

f. To promote and encourage the recognition and effective implementation of informational self-determination, as an essential prerequisite for the free development of the personality, with the aim of enabling individuals to decide, amongst other things, how they see themselves and how they wish to project themselves to others.

1.2. Human rights and gender perspective

a. The application and interpretation of legislation on the protection of personal data must be guided by a cross-cutting gender and human rights perspective, seeking to mitigate, as far as possible, any negative impact on individuals' rights, particularly those of people in vulnerable situations.

1.3. The relationship between regulation and the digital ecosystem

With a view to fostering the development of balanced and effective regulatory frameworks, efforts will be made to take the following parameters into account:

a. Regulatory consistency, whether by avoiding duplication between regulations or conceptual inconsistencies, particularly in the case of cross-cutting issues. The above is particularly relevant regarding the rules governing the digital ecosystem.

b. The impact of regulation in terms of avoiding disproportionate administrative burdens, with limited effectiveness.

c. The promotion of digital and algorithmic governance mechanisms to ensure the traceability, supervision, auditability and control of automated processing, artificial intelligence systems and other emerging or disruptive technologies.

2. Definitions

2.1. These Standards recommend the following definitions and their scope:

a. **Anonymisation:** a process by which personal data is processed with the aim of preventing the identification or re-identification of the data subject. It is irreversible because the data subject cannot reasonably be re-identified.

b. **Data Protection Authority:** a public institution of the State, of an administrative nature, endowed with full autonomy and independence to properly carry out its functions of supervising compliance

with the regulations, as well as safeguarding the effective exercise of data subjects' fundamental rights and freedoms.

c. **Consent:** a freely given, specific, unambiguous and informed expression of the data subject's wishes, by which they accept and authorise the processing of their personal data.

d. **Personal Data:** any information relating to an identified or identifiable natural person, expressed in numerical, alphabetic, graphic, photographic, alphanumeric, acoustic or any other form. A person is considered to be identifiable when their identity can be determined directly or indirectly, provided that this does not require disproportionate time or effort.

e. **Biometric data:** data obtained through specific technical processing and relating to the physical, physiological or behavioural characteristics of a natural person, which enable that person to be uniquely identified or their identity to be verified.

f. **Genetic data:** personal data relating to the inherited or acquired genetic characteristics of a natural person which provide unique information about that person's physiology or health, obtained in particular from the analysis of a biological sample from that person.

g. **Health data:** personal data relating to the physical or mental health of a natural person, including information on the provision of healthcare services, provided that such information reveals information about the data subject's state of health.

h. **Sensitive personal data or special categories of data:** personal data relating to the data subject's private sphere, or whose improper use may give rise to discrimination or entail a serious risk to the data subject. By way of example, this includes personal data that may reveal aspects such as a person's ethnic origin; religious, philosophical and moral beliefs or convictions; trade union membership; political opinions; health-related data; biometric data; neurodata; neural information from which personal, sensitive or emotional information may be inferred; sexual preference or orientation; genetic data; or biometric data intended to uniquely identify a natural person.

i. **Profiling:** the automated processing of personal data to evaluate certain personal aspects relating to a natural person, including, amongst other things, to analyse or predict aspects relating to that person's professional performance, financial situation, health, personal preferences, interests, reliability, behaviour, location or movements.

j. **Processor:** a service provider – whether a natural or legal person or a public authority – external to the controller's organisation, which processes personal data on the controller's behalf and for its account.

k. **Exporter:** a private natural or legal person, public authority, service, body or service provider situated within the territory of a State that carries out international transfers of personal data, in accordance with the provisions of these Standards.

l. **Scientific research:** any research that may support innovation, technological development and demonstration. These activities must contribute to existing scientific knowledge or apply existing knowledge in innovative ways; they must be carried out with the aim of contributing to the growth of general knowledge and the well-being of society; and they must comply with ethical standards in the relevant field of research. This does not rule out the possibility that the research may also serve a commercial purpose.

m. **Restriction of processing:** identification of the personal data to be retained for the purpose of restricting its processing thereafter, until such time as that measure is lifted or rendered ineffective.

n. **Neurodata:** data relating to the functioning, activity or structure of the human brain of a living natural person, including unique information about their physiology, health or mental states that can identify the data subject or make them identifiable.

ñ. **Controller:** a private natural or legal person, public authority, service or body which, alone or jointly with others, determines the purposes, means, scope and other matters relating to the processing of personal data.

o. **Pseudonymisation:** a process by which personal data are modified in such a way that they cannot be attributed to the data subject without additional information, provided that such additional information is held separately and is subject to security measures designed to ensure that the personal data cannot be attributed to an identified or identifiable natural person.

p. **Data subject:** a natural person to whom the personal data relate or pertain.

q. **Third party:** a natural person, legal person, authority, institution, public service or body, other than the data subject, the data controller and the data processor.

r. **Processing:** any operation or set of operations carried out on personal data using physical or automated means, including, but not limited to, the collection, access, recording, organisation, structuring, adaptation, indexing, modification, extraction, consultation, storage, retention, production, transfer, dissemination, possession, use and, in general, any use or disposal of personal data.

s. **Personal data breach:** any breach of security leading to the accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or to the unauthorised disclosure of or access to such data.

3. Subjective scope of application

3.1. These Standards are designed to serve as a framework applicable to individuals, private legal entities, public authorities and public bodies that process personal data in the course of their activities and functions.

4. Material scope of application

4.1. These Standards have been designed to serve as a framework applicable to the processing of personal data recorded on physical media, processed wholly or partly by automated means, or in both forms, irrespective of the manner or method of their creation, the type of medium, or the processing, storage and organisation of such data.

4.2. These Standards have been designed to serve as a framework applicable to the personal data of natural persons, in their capacity as data subjects.

4.3. The Standards were designed to serve as a framework within which the following circumstances are considered valid exceptions:

a) Where personal data is intended solely for activities within the context of a natural person's family or domestic life, that is to say, the use of personal data within a personal circle of friends, family members or close associates, and where such use is not intended for commercial disclosure or use.

b) Personal data that has undergone an effective anonymisation process.

4.4. National legislation in the Ibero-American States may provide for exceptions or limitations to compliance with the general framework for the protection of personal data.

In order to be legitimate, these exceptions or limitations must be designed exclusively as measures necessary in a democratic society to address threats to State security or public security and to prevent such threats, or to enable the competent authorities to prevent, investigate and prosecute criminal offences, as well as to enforce penalties.

In order to draft provisions designed to create exceptions correctly, the framework set out in section 6 of these Standards must be followed.

5. Territorial scope

5.1. The Standards recommend that the relevant national legislation be designed to apply to the processing of personal data carried out:

a. By a controller or processor established within the territory of the Ibero-American States.

b. By a controller or processor not established within the territory of the Ibero-American States, where the processing activities relate to the provision of goods or services aimed at residents of the Ibero-American States, or relate to the monitoring of their behaviour, insofar as this takes place within the Ibero-American States.

c. By a controller or processor who is not established in an Ibero-American State but to whom the national legislation of that State applies, as a result of entering into a contract or under public international law.

d. By a controller or processor not established within the territory of the Ibero-American States who uses or relies on means, whether automated or not, located within that territory to process personal data, unless such means are used solely for transit purposes.

5.2. For the purposes of these Standards, 'establishment' shall mean the place of the central or principal administration of the controller or processor, which must be determined on the basis of objective criteria and involve the effective and actual exercise of management activities that determine the main decisions regarding the purposes and means of the processing of personal data carried out, through stable arrangements.

5.3. The presence and use of technical means and technologies for the processing of personal data, or processing activities, shall not, in themselves, constitute a main establishment and shall not be regarded as decisive criteria for determining the main establishment of the controller or processor.

5.4. Where the processing of personal data is carried out by a group of companies, the principal establishment of the company which exercises control shall be deemed to be the principal establishment of the group, except where the purposes and means of the processing are effectively determined by another company within the group.

6. General exceptions to the right to personal data protection

6.1. The relevant national legislation of the Ibero-American States may limit the right to personal data protection in accordance with the provisions of section 4.4.

6.2. Exceptions and limitations shall be expressly recognised in a law, both in form and substance, with the aim of providing data subjects with sufficient certainty as to the nature and scope of the measure.

6.3. Should any of the Ibero-American States deem it necessary to provide for any exception or limitation to the right to personal data protection, it is recommended that the legislation in which such provisions are set out should include, as a minimum, provisions relating to:

a. The purpose of the processing.

b. The categories of personal data concerned.

c. The scope of the restrictions laid down.

d. Appropriate safeguards to prevent unlawful or disproportionate access or transfers.

e. Identification of the controller or controllers.

f. Retention periods for personal data.

g. Potential risks to data subjects' rights and freedoms.

h. The right of data subjects to be informed of the restriction, unless this would be detrimental to or incompatible with the purposes of the restriction.

6.4. Laws must be necessary, appropriate and proportionate in a democratic society, and must respect the fundamental rights and freedoms of data subjects.

7. Balancing the right to personal data protection

7.1. Ibero-American States may, in their constitutions, legislation or court rulings, provide for exceptions to compliance with certain principles or rights relating to the protection of personal data, solely to the extent that this is necessary to safeguard other fundamental rights and freedoms which so warrant and justify it, as might be the case with freedom of expression, freedom of the press and freedom of information, amongst others.

Exceptions must be applied strictly, with measures taken that are proportionate to the objectives pursued; any such restriction must always be justified and must be appropriate and proportionate in a democratic society.

7.2. This exemption must entail a balancing exercise to determine the necessity, suitability and proportionality of the restriction or exception in accordance with the rules and criteria laid down by the Ibero-American States in their domestic law.

8. Processing of personal data relating to children and adolescents: enhanced accountability

8.1. When processing personal data relating to children and adolescents, the Ibero-American States shall give priority to safeguarding their best interests, in accordance with the Convention on the Rights of the Child and other international instruments aimed at ensuring their well-being, respect for their progressive autonomy and comprehensive protection.

8.2. The Ibero-American States will promote:

a. In the education of children and adolescents, the responsible, appropriate and safe use of information and communication technologies and awareness of the potential risks they face in digital environments in relation to the improper processing of their personal data, as well as respect for their rights and freedoms.

b. The design and implementation of policies aimed at ensuring that information intended for minors is presented in clear, simple and accessible language so that they can understand the implications of the processing of their personal data.

8.3. The processing of personal data relating to children and adolescents must be subject to special measures involving enhanced accountability. The nature and intensity of such measures must be determined using a risk-based approach, in accordance with the child's best interests and their comprehensive protection.

The types of measures to be considered include protective default settings, access limitations, restrictions on profiling and behavioural advertising, effective age verification, where relevant; recommendation systems tailored to prevent harmful content; tools to block, mute and manage groups; and a ban on downloading and/or taking screenshots of content relating to minors, amongst others.

9. Processing of neurodata

9.1. The processing of neural data must be subject to special measures involving enhanced accountability. The nature and intensity of these measures must be determined using a risk-based approach.

When processing neural data, particular care must be taken to ensure compliance with the principles of data minimisation, accuracy, transparency, fairness, security and proactive accountability.

9.2. The following processing operations involving neural data are considered high-risk when their purpose is to:

a. Improperly infer mental states or innermost convictions.

b. Improperly influence people's will, decisions or behaviour.

c. Carry out mass surveillance in work, educational or government settings, for the purposes of control or monitoring.

d. Identify or authenticate individuals using neural patterns.

The processing operations described above could be subject to prohibitions under the legislation of the Ibero-American States.

10. Processing of sensitive personal data or special categories of data

10.1. The controller may not process sensitive personal data or special categories of data, unless one of the following exceptions applies:

a. The processing is essential for reasons of public interest; in such cases, the proportionality of the processing must be assessed in relation to the objective pursued, whilst essentially respecting the right to personal data protection and establishing appropriate measures to safeguard the data subject's fundamental rights and interests.

b. The processing relates to personal data which the data subject has manifestly made public.

c. The processing is necessary to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent.

d. The processing is necessary for the establishment, exercise or defence of claims, or where the courts are acting in the exercise of their judicial functions.

e. The processing is necessary for scientific or historical research purposes or for statistical purposes; in such cases, the proportionality of the processing must be assessed in relation to the objective pursued, whilst essentially respecting the right to personal data protection and establishing appropriate measures to safeguard the data subject's fundamental rights and interests.

f. The processing is essential for reasons of public interest in the field of public health, in response to serious cross-border threats to health, or to ensure adequate levels of quality and safety in

healthcare and in medicines or medical devices; appropriate measures must be taken to protect the rights and freedoms of the data subject.

g. Biometric data are necessary to confirm the identity of a data subject, provided that such biometric data, or the means necessary for verification, are under the exclusive control of the data subject.

10.2. The relevant national legislation of the Ibero-American States may provide for exceptions, safeguards and additional conditions to ensure the proper processing of sensitive personal data, in accordance with their domestic law.

Chapter II. Principles of personal data protection

11. Principles governing the processing of personal data

11.1. When processing personal data, the following principles must be observed: lawfulness, fairness, transparency, purpose limitation, data minimisation, data quality, proactive and demonstrable accountability, security and confidentiality.

These principles must be read, interpreted, applied and implemented in a manner that respects human dignity, in particular with a view to ensuring personal autonomy and physical and mental integrity, and to preventing the instrumentalisation of individuals or discrimination against them.

In any event, care must be taken to avoid disproportionate restrictions or adverse effects on individuals' autonomy and their treatment as mere instruments, particularly in the context of high-risk processing or processing involving the inference of sensitive or specially protected data. Any inferences, profiles, predictions or derived data generated as a result of the processing of personal data must be subject to appropriate safeguards regarding quality, relevance, proportionality and oversight.

12. Principle of lawfulness

12.1. The following are considered valid legal grounds for the processing of personal data:

a. The data subject gives their consent for one or more specific purposes.

b. The processing is necessary for compliance with a court order, decision or well-founded and reasoned directive from a competent public authority.

c. The processing is necessary for the exercise of the powers vested in public authorities or is carried out pursuant to a statutory authorisation.

d. The processing is necessary for the recognition or defence of the data subject's rights before a public authority.

e. The processing is necessary for the performance of a contract or a pre-contractual agreement to which the data subject is a party.

f. The processing is necessary for compliance with a legal obligation to which the controller is subject.

g. The processing is necessary to protect the vital interests of the data subject or of another natural person.

h. The processing is necessary for reasons of public interest laid down or provided for by law.

i. The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, in accordance with the applicable law in each country, provided that the following conditions are met:

   1) There must be a legitimate and lawful interest relating to actual activities; therefore, hypothetical situations do not qualify.

   2) It must have been assessed and determined that there are no reasonable alternatives that are equally effective and less intrusive for achieving the intended objectives. If there is a reasonable alternative that is equally effective, the legitimate interest does not apply.

   3) A balancing exercise must have been carried out to ensure that the individual interests, together with the fundamental rights and freedoms, of the data subjects do not take precedence over that legitimate interest. To this end, consideration must be given to the data subjects' interests, the impact of the processing and their reasonable expectations, as well as the existence of additional safeguards that could limit the impact on the data subject. During this balancing exercise, particular care must be taken if the data subject is a child or adolescent.

State authorities, institutions, bodies, agencies or public services shall not be permitted to use legitimate interest as a legal basis for the processing of personal data in the exercise of their functions or powers.

13. Conditions for consent

13.1. Where it is necessary to obtain the data subject's consent, the controller shall demonstrate beyond doubt that the data subject gave their consent, either through a statement or a clear affirmative action.

13.2. Where consent is given in the context of a written statement that also relates to other matters, the request for consent must be presented in such a way that it is clearly distinguishable from those other matters, in a comprehensible and easily accessible manner, and using clear and plain language. Any consent obtained through practices that contravene the applicable regulations shall be invalid.

13.3. Whenever consent is required for the processing of personal data, the data subject may withdraw their consent at any time; to this end, the controller shall put in place simple, swift, effective and free-of-charge mechanisms.

14. Consent for the processing of personal data relating to children and adolescents

14.1. When obtaining consent from children and adolescents, the controller shall obtain authorisation from the holder of parental authority or guardianship, in accordance with the rules on representation laid down in the domestic law of the Ibero-American States, or, where applicable, shall seek authorisation directly from the minor if the domestic law of each Ibero-American State has established a minimum age at which the minor may grant such authorisation directly, without any representation by the holder of parental authority or guardianship. Any consent obtained in a manner contrary to the provisions set out herein shall be deemed unlawful.

14.2. The controller shall make reasonable efforts to verify that consent was given by the holder of parental authority or guardianship, or by the child directly, depending on their age, in accordance with the domestic law of each Ibero-American State, considering the technology available.

14.3. Processing for the purposes of creating profiles for advertising purposes would, where applicable, require specific consent, separate from consent for other processing operations.

15. Principle of fairness

15.1. The controller shall process the personal data in its possession, prioritising the protection of the data subject's interests and refraining from processing such data by deceptive or fraudulent means.

15.2. For the purposes of these Standards, any processing of personal data that gives rise to unfair or arbitrary discrimination against data subjects shall be deemed unfair.

16. Principle of transparency

16.1. The controller shall inform the data subject of the existence and main characteristics of the processing to which their personal data will be subject, so that they may make informed decisions in this regard.

16.2. The data subject is entitled, at the very least, to be informed of the following:

a. The controller's identity and contact details.

b. The categories, classes or types of data subject to processing.

c. The lawful basis on which the processing is carried out.

d. The purposes for which their personal data will be processed.

e. The contact details of the data protection officer, where applicable.

f. The legitimate interest pursued, as well as the information necessary to provide data subjects with assurance that their fundamental rights and freedoms are not adversely affected by processing

based on legitimate interests. This applies only where legitimate interests form the legal basis for the processing.

g. Any disclosures of personal data, whether domestic or international, that the controller intends to make, including the recipients and the purposes for which such disclosures are being made.

h. The data retention period. If it is not possible to specify the timeframe, the criteria used to determine it.

i. The existence, form and mechanisms or procedures through which the data subject may exercise their rights of access, rectification, erasure or the right to be forgotten, objection, data portability, restriction of processing and the right not to be subject to automated decision-making.

j. The existence of automated decisions accompanied by information that is useful to data subjects regarding the logic applied, the relevance of the processing and its consequences, set out in clear, simple and easily understandable language. Furthermore, where relevant, data subjects will be informed about profiling, the sources of reference data and the main consequences of such processing. Where artificial intelligence systems are used, meaningful information must be provided on the system's role in decision-making, the extent of automation involved, the main variables or criteria used, and the system's relevant limitations.

k. Where applicable, the source of the personal data where the controller has not obtained the data directly from the data subject.

16.3. The information provided to data subjects must be sufficient and easily accessible, and must be drafted and structured in clear, simple language that is easy for the data subjects to whom it is addressed to understand, particularly in the case of children and adolescents.

16.4. Every controller must have transparent policies governing the processing of personal data that they carry out.

17. Principle of purpose limitation

17.1. Any processing of personal data shall be limited to the fulfilment of specific, explicit and legitimate purposes.

17.2. The controller may not process the personal data in its possession for purposes other than those for which they were originally processed, unless one of the grounds authorising further processing in accordance with the principle of lawfulness applies.

The processing of data for purposes other than those for which the processing was originally carried out shall be permissible provided that an assessment is carried out beforehand to verify that such purposes are compatible with those for which the processing was originally carried out. When assessing compatibility, the following factors must be taken into account:

a. The link between the original purpose and the new one.

b. The nature of the data, particularly where sensitive data is involved.

c. The context in which the data were collected.

d. The existence of technical and organisational safeguards for the benefit of data subjects.

e. The reasonable expectations of data subjects.

f. The existence of appropriate measures relating to governance, traceability and the protection of rights, particularly where data are intended to be reused for the training, fine-tuning, validation or improvement of automated systems or artificial intelligence systems.

This provision shall not apply to processing based on consent.

17.3. The further processing of personal data for archiving purposes, for scientific and historical research, or for statistical purposes – all of which are in the public interest – shall not be regarded as incompatible with the original purposes.

17.4. In the case of the processing of minors' personal data for a new purpose, the protection of children's rights must be given the same priority as when the data were first collected.

18. Principle of data minimisation

18.1. The controller shall process only personal data that are adequate, relevant and limited to what is necessary in relation to the purposes that justify their processing. The use of automated technologies or artificial intelligence systems shall not, in itself, justify the mass, indiscriminate or disproportionate collection of personal data.

19. Principle of data quality

19.1. The controller shall take the necessary measures to ensure that the personal data in its possession are accurate, complete, relevant and up to date, so as not to compromise their truthfulness, reliability or suitability for the purposes for which they were processed. The quality of personal data must be assessed considering the nature, context, purposes and potential effects of the processing on individuals' rights and freedoms.

In the case of automated processing, including that carried out using artificial intelligence systems, the controller must take reasonable measures to ensure the quality, relevance, representativeness, integrity and up-to-date status of the data used throughout the system's life cycle, including data used for training, validation, testing, fine-tuning, input, monitoring and operation.

It must also put in place governance and oversight mechanisms designed to prevent or mitigate undue bias, inaccurate inferences, arbitrary discrimination, erroneous associations, a decline in data quality, or results that are manifestly false, inaccurate, disproportionate or misleading, or that arise from incomplete, out-of-date, unrepresentative or decontextualised data.

Where processing involves profiling, predictive systems or artificial intelligence, the controller must periodically assess the reliability, relevance, accuracy, proportionality and quality of the inferences,

classifications, recommendations, predictions or results generated by the system, particularly where these may produce legal effects or have a significant impact on individuals.

19.2. Where personal data are no longer necessary for the purposes for which they were processed, the controller shall delete or remove them from its files, records, databases, dossiers or information systems, or, where appropriate, subject them to an anonymisation process. In the case of automated processing, including that carried out by artificial intelligence systems, the controller must take reasonable measures to prevent the incompatible reuse, undue persistence or disproportionate retention of personal data and inferences derived from them.

19.3. When deleting personal data, the controller shall implement methods and techniques designed to ensure the permanent and secure deletion of such data.

19.4. Personal data shall only be retained for as long as is necessary to fulfil the purposes justifying their processing or those relating to legal requirements applicable to the controller.

However, the relevant national legislation of the Ibero-American States may provide for exceptions regarding the retention period for personal data, whilst fully respecting the rights and safeguards of the data subject.

20. Principle of proactive and demonstrable accountability

20.1. The controller shall implement technical and organisational measures, proportionate to the risk, to demonstrate compliance with data protection legislation.

When assessing risk, account must be taken of the nature, scope, context and purposes of the processing, as well as the likelihood and severity of any adverse effects on data subjects' fundamental rights and freedoms.

Certifications, binding corporate rules, codes of conduct or similar schemes may serve to demonstrate compliance, provided that the aforementioned mechanisms possess the following attributes: they are recognised by a Personal Data Protection Authority, such recognition is based on independent and accredited supervision, and they are transparent and publicly verifiable mechanisms.

20.2. The above shall apply where personal data are processed by a processor on behalf of and for the account of the controller, as well as when personal data are transferred.

20.3. The measures that the controller may adopt to comply with the principle of accountability include, by way of example but not limited to, the following:

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

b. Implement risk management systems relating to the processing of personal data.

c. Draw up mandatory and enforceable personal data protection policies and programmes within the controller's organisation.

d. Implement a programme to train and update staff on their obligations regarding the protection of personal data.

e. Periodically review personal data security policies and programmes to identify any necessary changes.

f. Establish a system of internal and/or external monitoring and oversight, including audits, to verify compliance with personal data protection policies.

g. Establish procedures for receiving and responding to queries and complaints from data subjects.

h. Maintain reasonable mechanisms for governance, traceability, documentation, the recording of relevant decisions, oversight, control and risk management, including, where appropriate, mechanisms for effective human oversight and periodic review of impacts.

20.4. The controller shall continuously review and assess the mechanisms voluntarily adopted to comply with the principle of accountability, with a view to measuring their effectiveness in ensuring compliance with applicable national legislation.

21. Principle of security

21.1. The controller and the processor shall, irrespective of the type of processing carried out, implement and maintain appropriate administrative, physical and technical measures to ensure a level of security appropriate to the risk involved. These measures shall include, where applicable, measures to ensure the ongoing confidentiality, integrity, resilience and availability of processing systems and services; the pseudonymisation and encryption of data; and the ability to restore the availability of and access to personal data promptly following a physical or technical incident.

21.2. In determining the measures referred to in the preceding paragraph, the controller shall take the following factors into account:

a. The risk to data subjects' rights and freedoms, particularly in view of the potential quantitative and qualitative value that the personal data being processed may have for an unauthorised third party.

b. The state of the art.

c. Implementation costs.

d. The nature of the personal data processed, where sensitive personal data is involved.

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

f. Any international transfers of personal data that are carried out or intended to be carried out.

g. The number of data subjects.

h. The potential consequences for data subjects in the event of a personal data breach.

i. Previous personal data breaches relating to the processing of personal data.

21.3. The controller and the processor shall carry out a series of actions to ensure the establishment, implementation, operation, monitoring, review, maintenance and continuous improvement of the security measures applicable to the processing of personal data, on a regular basis.

The controller and the processor shall implement measures to ensure that any person acting under their authority in the processing of personal data is obliged to comply with the instructions and commitments designed to ensure security throughout the entire data processing chain.

In automated processing operations, including those carried out using artificial intelligence systems, these measures must include, where relevant, data integrity controls, version control, operational monitoring, protection against system tampering and mitigation of unintended behaviour.

22. Notification of personal data breaches

22.1. Where the controller becomes aware of a personal data breach occurring at any stage of the processing, it shall notify the Personal Data Protection Authority of such an incident without delay, unless, following an assessment, it is determined that the breach does not pose a risk to the rights and freedoms of data subjects.

The notification that the controller submits to the Personal Data Protection Authority must include at least the following information:

a. The nature of the personal data breach.

b. The potential consequences of the personal data breach.

c. The measures taken or proposed by the controller to remedy the aforementioned breach.

d. Measures designed to mitigate any potential adverse effects, where applicable.

The processor must notify the controller, without delay, of any personal data breaches of which it becomes aware.

22.2. Data subjects must be notified of any personal data breaches that pose a high risk to their rights and freedoms. The controller must give notice without undue delay.

22.3. The notification sent by the controller to the data subjects concerned shall be written in clear and plain language.

22.4. The notification sent by the controller to the data subject shall contain at least the following information:

a. The nature of the incident.

b. The personal data that have been compromised.

c. Corrective actions taken immediately.

d. Recommendations to the data subject regarding the measures they may take to protect their interests.

e. The channels available to the data subject for obtaining further information on this matter.

22.5. The controller shall document any personal data breach occurring at any stage of the processing, identifying, by way of example but not limited to, the date on which it occurred; the cause of the breach; the facts relating to it and its effects; and the corrective measures implemented immediately and definitively. Such documentation shall be made available to the supervisory authority.

22.6. The relevant national legislation of the Ibero-American States shall set out the effects of notifications of personal data breaches made by the controller to the supervisory authority, in terms of the procedures, form and conditions of the authority's intervention, with the aim of safeguarding the interests, rights and freedoms of the data subjects concerned.

23. Principle of confidentiality

23.1. The controller shall put in place controls or mechanisms to ensure that those involved in any stage of the processing of personal data maintain and respect the confidentiality of such data; this obligation shall continue even after their relationship with the data subject has ended.

This does not prevent the communication and transfer of personal data from taking place in accordance with the provisions of the applicable legislation.

Chapter III. Rights of the data subject

24. Rights

24.1. At any time, the data subject or their representative may request from the controller access to, rectification of, erasure of their personal data and the right to be forgotten, object to processing, not to be subject to decisions based exclusively or essentially on automated processing, obtain the portability of their personal data, and restrict the processing of data relating to them.

24.2. The exercise of any of the rights referred to in the preceding paragraph is not a prerequisite for, nor does it prevent the exercise of, any other right.

25. Right of access

25.1. The data subject shall have the right to request access to their personal data held by the controller, as well as to obtain any information relating to the general and specific conditions governing the processing of that data.

26. Right to rectification

26.1. The data subject shall have the right to obtain from the controller the rectification or correction of their personal data where such data are inaccurate, incomplete or not up to date.

27. Right to erasure and right to be forgotten

27.1. The data subject shall have the right to request the erasure of their personal data from the controller, so that such data are erased without delay in the following cases:

a. The data are no longer necessary for the purposes for which they were obtained.

b. The data subject withdraws their consent, where the processing was based on that consent.

c. The data subject has objected to the processing in accordance with section 28.1(a), and no other legitimate grounds prevail, or the data subject objects in accordance with section 28.1(b).

d. The data have been processed unlawfully.

In the event that personal data have been made public, particularly in digital environments, and the controller is obliged to erase the data in accordance with any of the cases described, they must inform the other controllers processing the data of the request to remove any link to those data, or to any copy or replica thereof. The exercise of this right may be lawfully restricted where the processing is essential for the exercise of freedom of expression and information, compliance with a legal obligation, reasons for public interest, scientific or historical research or statistical purposes, and for the establishment, exercise or defence of legal claims.

28. Right to object

28.1. The right to object may only be exercised where the processing has taken place in the performance of a task carried out in the public interest or in the exercise of official functions or powers, or for the purposes of pursuing legitimate interests.

The data subject may exercise their right to object:

a. For reasons relating to their particular situation, including profiling. The controller must cease processing unless it can demonstrate compelling legitimate grounds that override the data subject's fundamental rights and freedoms, or the processing is necessary for the establishment, exercise or defence of legal claims.

b. Where the processing of their personal data is for the purposes of direct marketing, including profiling, insofar as it relates to that activity.

28.2 With regard to the preceding paragraph, where the data subject objects to the processing of their personal data for direct marketing purposes, their personal data shall no longer be processed for such purposes.

28.3. Where the processing of personal data has been carried out on the basis of the controller's legitimate interests, in the context of the development and operation of an artificial intelligence system, the data subject's right to object shall be unconditional.

The controller must put in place reasonable governance, traceability and control measures designed to facilitate the effective exercise of this right, taking into account the nature of the processing and those cases in which the erasure, de-linking or complete cessation of the use of personal data or of inferences derived from them is not technically or materially feasible.

29. Right not to be subject to automated individual decision-making

29.1. The data subject shall have the right not to be subject to decisions which produce legal effects or significantly affect them where such decisions are based solely or predominantly on automated processing, including processing carried out by artificial intelligence systems designed to evaluate, classify, recommend, profile, analyse or predict personal aspects of the data subject.

Children and adolescents must not be subject to decisions that produce legal or significant effects based solely on automated processing, unless enhanced safeguards are in place.

29.2. The provisions of the preceding paragraph shall not apply where the automated processing of personal data is necessary for the conclusion or performance of a contract between the data subject and the controller; is authorised by the domestic law of the Ibero-American States; or is based on the data subject's demonstrable consent.

29.3. However, where necessary for the contractual relationship or where the data subject has given their consent, they shall have the right to meaningful and effective qualified human intervention, involving a genuine ability to understand the main principles of the system, to critically evaluate its results and to reasonably deviate from them; to receive a meaningful and clear explanation of the logic applied, so that they may understand the main criteria and determining factors underlying the decision taken; the significance and main consequences of such processing for them; and to express their point of view and challenge the decision.

29.4. The controller shall not carry out automated processing of personal data which results in discrimination against data subjects on the grounds of their origin; religious, philosophical or moral beliefs or convictions; trade union membership; political opinions; data relating to health, life, neural data, sexual preference or orientation, as well as genetic data or biometric data.

30. Right to data portability

30.1. Where personal data are processed electronically or by automated means, the data subject shall have the right to obtain a copy of the personal data they have provided to the controller or which are being processed, in a structured, commonly used and machine-readable electronic format (interoperable format), enabling them to continue using such data and to transfer them to another controller, should they so require

This right may be exercised only if:

a. The processing is carried out exclusively by automated means.

b. The processing is based on consent or on a contract.

30.2. The data subject may request that their personal data be transferred directly from one controller to another where this is technically feasible.

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

30.4. Without prejudice to the data subject's other rights, the right to data portability shall not apply to information that has been inferred, derived, created, generated or obtained from the analysis or processing carried out by the controller on the basis of the personal data provided by the data subject, such as personal data that have undergone a process of personalisation, recommendation, categorisation or profiling.

31. Right to restriction of processing of personal data

31.1. The data subject shall have the right to restrict the processing of personal data in the following cases:

a. The data subject exercises their right to rectification for the period necessary to enable the controller to give effect to that right.

b. The data subject objects to the processing of their data, for as long as it takes the controller to establish the existence of compelling legitimate interests that override those of the data subject.

c. The data subject requests that the data not be erased where their data have been processed unlawfully, in order to exercise or defend their rights.

The data subject requests restriction for the purpose of establishing, exercising or defending legal claims, in the case of data that have fulfilled their purposes.

31.2. Data subjects shall be informed before the restriction of processing is lifted in all cases.

32. Exercise of rights relating to the protection of personal data

32.1. The controller shall put in place simple, expeditious, accessible and free means and procedures to enable data subjects to exercise their rights of access, rectification, erasure, objection and data portability.

32.2. The relevant national legislation of the Ibero-American States shall set out the requirements, time limits, terms and conditions under which data subjects may exercise their rights of access, rectification, erasure, objection and data portability, as well as the grounds on which the exercise of such rights may be inadmissible, including, but not limited to, the following:

a. Where processing is necessary for the fulfilment of an important public interest objective.

b. Where processing is necessary for the performance of the functions of public authorities.

c. Where the controller demonstrates that there are legitimate grounds for the processing to take precedence over the data subject's interests, rights and freedoms.

d. Where processing is necessary to comply with a legal provision.

e. Where personal data are necessary for the maintenance or fulfilment of a legal or contractual relationship.

32.3. The relevant national legislation of the Ibero-American States may recognise that natural persons connected with deceased individuals, or designated by them, may exercise the rights referred to in this Standard in respect of the personal data of deceased individuals that concern them.

32.4. The relevant national legislation of the Ibero-American States shall recognise the data subject's right to challenge or contest the responses provided by the controller in response to a request to exercise the rights referred to in this section, or the controller's failure to respond, before the supervisory authority and, where appropriate, before the courts, in accordance with the domestic law of each Ibero-American State.

32.5. Alternative dispute resolution mechanisms may be used, provided that judicial review is guaranteed, that they are a voluntary and impartial alternative, and that they do not preclude recourse to the courts. The Personal Data Protection Authority must supervise compliance with these conditions in order to recognise the validity of the actions carried out through these mechanisms.

Chapter IV. Processor

33. Scope of the processor's responsibilities

33.1. The processor shall carry out personal data processing activities without having any decision-making power regarding the scope and content of such processing, and shall limit its actions to the terms set by the controller.

34. Formalisation of the processor's provision of services

34.1. The provision of services between the controller and the processor shall be formalised by the signing of a contract or any other legal instrument provided for by the Ibero-American States in their relevant national legislation.

34.2. The contract or legal instrument shall set out, at a minimum, the subject matter, scope, content, duration, nature and purpose of the processing; the type of personal data; the categories of data subjects; and the obligations and responsibilities of the controller and the processor.

34.3. The contract or legal instrument shall set out, at the very least, the following general clauses relating to the services to be provided by the processor:

a. Process personal data in accordance with the instructions of the controller.

b. Refrain from processing personal data for purposes other than those specified by the controller.

c. Implement security measures in accordance with the relevant legal instruments.

d. Notify the controller of any personal data breach involving data processed on its instructions.

e. Maintain the confidentiality of the personal data processed.

f. Erase, return or disclose the personal data being processed to a new processor appointed by the controller, once the legal relationship with the controller has ended or on the controller's instructions, unless a statutory provision requires the retention of the personal data, or the controller authorises the disclosure of such data to another processor.

g. Refrain from transferring personal data, except where the controller so determines, or where the disclosure arises from subcontracting, or by express order of the supervisory authority.

h. Allow the controller and the supervisory authority to carry out inspections and checks at the processor's premises and facilities.

i. Prepare, update and retain the necessary documentation to demonstrate compliance with its obligations.

j. Cooperate with the controller on all matters relating to compliance with the relevant national legislation of the Ibero-American State.

k. Where the service involves automated systems, artificial intelligence or other emerging technologies, provide the controller with sufficient information regarding the general functioning of the system, its relevant limitations, security measures, traceability, data quality, monitoring and risk management, to the extent necessary to enable the controller to fulfil its obligations.

34.4. Where the processor fails to comply with the instructions of the controller and decides on its own regarding the scope, content, means and other aspects of the processing of personal data, it shall assume the status of controller, in accordance with the relevant national legislation of the Ibero-American State applicable in this matter.

35. Subcontracting of services

35.1. The processor may, in turn, subcontract services involving the processing of personal data, provided that there is prior written authorisation – whether specific or general – from the controller, or that this is expressly stipulated in the contract or legal instrument entered into between the controller and the processor.

35.2. The sub-processor shall act as a processor in accordance with the terms set out in the relevant national legislation of the Ibero-American State.

35.3. The processor shall formalise the provision of services by the sub-processor by means of a contract or any other legal instrument as determined by the national legislation of the Ibero-American State applicable in this matter.

35.4. Where the sub-processor fails to fulfil its obligations and responsibilities in relation to the processing of personal data carried out in accordance with the instructions of the processor, it shall assume the role of controller in accordance with the relevant national legislation of the Ibero-American State applicable in this matter.

Chapter V. International transfers of personal data

36. General rules for international transfers of personal data

The only international transfers of personal data considered valid under these Standards shall be those carried out by controllers and processors in accordance with the rules set out in this section.

The controller or processor may carry out international transfers of personal data in any of the following circumstances:

a. A third country, part of its territory, sector or activity, or an international organisation, has been recognised by the country from which the data are to be exported as having an adequate level of personal data protection.

For the purposes of recognising an adequate level of protection, Personal Data Protection Authorities must assess at least the following aspects:

1) The rule of law, specifically respect for fundamental rights and individual freedoms; the relevant legislation on the protection of personal data, both general and sector-specific; legislation on national security, public security and criminal matters; and legislation governing access to personal data by State authorities, with the aim of verifying the level of equivalence between the two countries in the areas described.

2) The existence and effective functioning of one or more Personal Data Protection Authorities, and verification that such authority or authorities meet the design and characteristics set out in paragraph 42 of the Standards.

3) The existence of individual rights that data subjects can effectively exercise before Personal Data Protection Authorities and the competent courts.

4) The international commitments to which the third country or international organisation is a party, in order to ascertain the scope of its commitments in relation to personal data.

Once the assessment has been completed, a decision may be taken on whether or not to recognise a third country or international organisation as having an adequate level of protection. The document adopting a favourable recognition decision must set out a mechanism for periodic review to ensure that the conditions remain in place over time. The review must be carried out at least every 5 years.

b. Where the third country or international organisation to which an international transfer of personal data is to be made has not been recognised by the country from which the data are to be exported as having an adequate level of protection, the controller or processor may provide appropriate safeguards through the following instruments:

1) Standard data protection clauses adopted by the Personal Data Protection Authority, which controllers and processors may adhere to, thereby ensuring compliance with the data protection legislation of the country from which the data are exported.

2) Binding and enforceable codes of conduct, representing an association or sectoral body, subject to independent and effective oversight mechanisms, which ensure compliance with the data protection legislation of the country from which the data are exported and which must be assessed and approved by the Personal Data Protection Authority of that country.

3) Binding corporate rules which ensure and demonstrate compliance with the data protection legislation of the country from which the data are exported, and which have been reviewed and approved by the Personal Data Protection Authority of that country.

4) Certifications which ensure and demonstrate compliance with the data protection legislation of the country from which the data are exported, and which have been reviewed and approved by the Personal Data Protection Authority of that country.

5) Legally binding and enforceable instruments between State institutions and public bodies.

6) Contractual clauses between a controller or processor in the country from which the data are exported and a recipient in a third country or international organisation. These clauses must be authorised by the Personal Data Protection Authority in order to be valid.

c. In the absence of an adequacy decision or appropriate safeguards, international transfers of personal data may be carried out in the following exceptional cases:

1) The data subject has expressly consented to the transfer after being informed of the potential risks involved.

2) The transfer is essential for the conclusion or performance of a contract, or for pre-contractual measures, relating to the data subject.

3) For reasons of public interest.

4) For the establishment, exercise or defence of legal claims.

5) To protect the vital interests of the data subject or of a third party, where the data subject is unable to give their consent.

6) The transfer is made from a public register whose purpose is to provide information and which is open to consultation by the general public or by any person who can demonstrate a legitimate interest, solely to the extent that the requirements laid down in the applicable legislation for such consultation are met.

The cases described in points 1) and 2) shall not apply to activities carried out by public authorities and institutions of the State in the exercise of their public functions, powers or authority.

d. Where an international transfer of personal data cannot be carried out using any of the mechanisms described in sub-paragraphs (a), (b) and (c), it may be carried out on an exceptional basis, provided that all of the following conditions are met:

1) The transfer is not repetitive.
2) The transfer concerns a limited number of data subjects.
3) The transfer is necessary for the compelling legitimate interests of the controller, which override the rights and freedoms of the data subjects. The data subject must be informed of these legitimate interests.
4) The controller has provided appropriate safeguards in the circumstances.
5) The Personal Data Protection Authority is notified.

Exception (d) shall not apply to activities carried out by public authorities and institutions of the State in the exercise of their public functions, powers or authority.

Chapter VI. Proactive measures in the processing of personal data

37. Recognition of proactive measures

37.1. The national legislation of the Ibero-American States applicable in this area may recognise and establish measures that promote better compliance with that legislation and help to strengthen and improve the personal data protection controls implemented by the controller. These may include the measures set out below in this Chapter.

38. Privacy by design and privacy by default

38.1. The controller shall implement preventive measures of various kinds, from the design stage onwards, when determining the means of processing personal data, during the processing itself and before collecting personal data, to ensure the effective application of the principles, rights and other obligations laid down in the national legislation of the relevant Ibero-American State. In the case of automated processing, including that carried out using artificial intelligence systems, the measures must provide for reasonable mechanisms for supervision, traceability, documentation, risk management and monitoring of the system's operation, considering the nature, context and potential effects of the processing.

38.2. The controller shall ensure that its programmes, services, IT systems or platforms, electronic applications or any other technology involving the processing of personal data comply by default with, or conform to, the principles, rights and other obligations laid down in the national legislation of the relevant Ibero-American State. Specifically, this is intended to ensure that only the minimum amount of

personal data is processed and that access to such data, without the data subject's involvement, is restricted to an indeterminate number of people.

39. Data Protection Officer

39.1. The controller and the processor shall appoint a Data Protection Officer, taking into account their professional training and experience, their specialised and duly accredited knowledge in the field of personal data protection, and their ability to perform the duties described in paragraph 39.4.

The appointment of a Data Protection Officer shall be mandatory in the following cases:

a. Where the controller or processor is a public authority. For the purposes of this provision, a public authority is not only one that forms part of the State in the strict sense, but also private entities that carry out activities typically performed by the State through concessions, permits or authorisations, amongst other means.

b. Where the controller or processor carries out processing of personal data for the purpose of regularly and systematically monitoring the data subject's behaviour.

c. Where the controller or processor carries out processing of personal data that is likely to entail a high risk to data subjects' right to personal data protection, taking into account, amongst other factors and by way of example but not limitation, the categories of personal data processed, particularly where sensitive data is involved; any transfers carried out; the number of data subjects; the scope of the processing; the information technologies used; and the purposes of such processing.

39.2. A controller who does not fall within any of the grounds set out in the preceding paragraph may appoint a Data Protection Officer if they deem it appropriate.

39.3. The controller shall be obliged to support the Data Protection Officer in the performance of their duties, providing them with the necessary resources to carry out those duties and to maintain and update their specialist knowledge.

39.4. The Data Protection Officer shall have at least the following duties:

a. To advise the controller or processor on matters submitted for their consideration relating to the protection of personal data.

b. To coordinate, within the organisation of the controller or processor, the policies, programmes, measures and other relevant activities required to ensure compliance with personal data protection requirements.

c. To monitor compliance with personal data protection requirements within the organisation, under the responsibility of the controller or processor.

d. To cooperate with the Personal Data Protection Authority and act as its point of contact.

39.5. The controller and the processor shall ensure that the Data Protection Officer does not receive instructions regarding the performance of their duties, and that they do not find themselves in situations of conflict of interest arising, where applicable, from other activities within the organisation. The Data Protection Officer shall report to senior management or to the highest authority of the controller or processor.

40. Self-regulatory mechanisms

40.1. The controller may voluntarily adhere to binding self-regulatory schemes, the purpose of which is, amongst other things, to contribute to the correct application of the relevant national legislation of the Ibero-American State and to establish procedures for resolving disputes between the controller and the data subject, without prejudice to other mechanisms established by the relevant national legislation, taking into account the specific characteristics of the personal data processing carried out, as well as the effective exercise and respect for the data subject's rights.

40.2. For the purposes of the preceding paragraph, codes of professional ethics and certification schemes – and their respective trust seals – may be developed, amongst other measures, to help achieve the objectives set out in this paragraph.

40.3. The relevant national legislation of the Ibero-American States shall lay down the appropriate rules for the validation, confirmation or recognition of the self-regulatory mechanisms referred to above.

41. Data protection impact assessment

41.1. Where the controller intends to carry out a particular type of personal data processing, particularly using emerging or disruptive technologies, including artificial intelligence systems, biometric technologies, neurotechnologies, predictive systems and other technologies capable of producing intensive, inferential or highly automated processing of personal data, which, by virtue of its nature, scope, context or purposes, is likely to result in a high risk to the rights and freedoms of data subjects, the controller shall, prior to the processing, carry out an assessment of the impact of the processing operations on the protection of personal data.

The assessment must include at least the following:

a. A systematic description of the processing operations intended to be carried out, their purposes and, where applicable, the legitimate interests pursued by the controller.

b. An assessment of the necessity and proportionality of the processing operations to be carried out, in relation to their purposes.

c. An assessment of the risks to the rights and freedoms of data subjects.

d. The measures envisaged to address the risks. This section of the assessment must set out all the safeguards and mechanisms designed to ensure and demonstrate the protection of personal data and compliance with the relevant legislation.

e. A description of algorithmic governance measures, and the measures envisaged for the supervision, traceability, control and mitigation of risks associated with automated or artificial intelligence systems.

Where appropriate, the controller shall seek the data subjects' views on the processing to be carried out, without prejudice to any public, commercial or security interests that may be involved.

41.2 It is recommended that a data protection impact assessment be carried out in the following cases:

a. Automated processing or processing based on artificial intelligence systems, including profiling, which generate recommendations or decisions that are exclusively or predominantly automated, and which may produce legal effects, similarly significant effects, or significantly influence the behaviour, decisions, access to rights, opportunities, essential services or living conditions of natural persons.

b. Large-scale processing of sensitive data or special categories of data.

c. The high-risk processing operations described in these Standards.

d. Processing operations involving systematic observation on a large scale in areas open to the public.

e. International transfers of personal data to countries that have not been recognised as providing an adequate level of protection, provided that it is not possible to offer any of the appropriate safeguards recognised in paragraph 36.1(b), or that the existence of any of the exceptions set out in paragraph 36.1(c) cannot be demonstrated.

Where the outcome of the data protection impact assessment indicates that the processing may pose a high risk if appropriate mitigation measures are not implemented, the controller shall be obliged to consult the Personal Data Protection Authority before commencing the processing.

The aim of this consultation is for the Personal Data Protection Authority to advise the controller. To this end, the controller must provide the Personal Data Protection Authority with the data protection impact assessment carried out, as well as any other information that may be required.

Chapter VII. Personal Data Protection Authorities

42. Personal Data Protection Authorities

42.1. Data protection legislation must provide for the establishment of one or more Personal Data Protection Authorities, with the aim of monitoring and ensuring compliance with the regulations, as well as guaranteeing respect for individuals' rights and freedoms.

42.2. Personal Data Protection Authorities must be granted full autonomy under the legislation and regulations governing them. Full autonomy must, as a minimum, ensure that they fulfil their objectives and exercise their functions, responsibilities, authority and powers impartially and independently, free

from any external influence, whether direct or indirect, and without requiring or accepting any orders or instructions.

Although the highest degree of autonomy recognised by the legal system of each Ibero-American State might prove to be the most effective framework for the design of such authorities, in cases where this is not feasible, they may be granted functionally effective autonomy that ensures they can fulfil their objectives and fully exercise their functions.

42.3. The authorities may have a single individual or a collegiate body at the head of their highest governing body.

The member or members of the authorities' governing bodies must have experience and specialist knowledge of law and personal data protection, particularly in the areas of regulatory oversight and international cooperation.

The selection procedure must be transparent and ensure its impartiality and credibility, as well as guarantee that the selection is based primarily on technical qualifications and merit.

The appointed person or persons may only be removed from office on serious grounds laid down in national legislation, in accordance with the rules of due process, or if they cease to meet the conditions required to perform their duties.

Any member or members of the authority's governing bodies must refrain from any action that is incompatible with their responsibilities throughout their term of office.

42.4. In addition to the functions set out throughout the Standards, Personal Data Protection Authorities must have the appropriate powers, authority, jurisdiction and competence to achieve their objectives.

The structure of the Personal Data Protection Authorities must be set out in legislation in such a way as to enable them, at a minimum, to exercise the following powers and perform the following functions:

a. Investigate, monitor or oversee compliance with the regulations.

b. Order provisional, proportionate and reviewable interim measures as a preventive and urgent measure.

c. Issue rulings.

d. Impose sanctions for infringements.

e. Ensure that data subjects' rights are effectively upheld.

f. Issue regulations.

g. Interpret the regulations.

h. Design and implement public policies.

i. Design and implement capacity-building programmes.

j. Build and foster a culture of data protection.

k. Create and promote knowledge.

I. Cooperate internationally with other authorities.

In carrying out their duties, Personal Data Protection Authorities must implement policies designed to provide appropriate support for vulnerable groups, in accordance with their needs, thereby enabling them to exercise their rights effectively.

42.5. The decisions and actions of the Personal Data Protection Authority, taken exclusively in the exercise of its functions, powers, authority and jurisdiction, shall be subject to judicial review. National legislation must therefore include the necessary provisions to ensure such review.

42.6. Personal Data Protection Authorities must have the necessary human and material resources to carry out their duties.

Each Ibero-American State must ensure that the financial controls to which the Personal Data Protection Authority is subject do not undermine its full autonomy and independence. It must therefore have a public budget, irrespective of any other sources of funding it may have.

Furthermore, it must be ensured that each authority is free to appoint and manage its own staff, and that such staff report exclusively to the governing body of the Personal Data Protection Authority.

Chapter VIII. Complaints and sanctions

43. Complaints procedure and sanctions regime

43.1. Every data subject shall have the right to lodge a complaint with the Personal Data Protection Authority, as well as to seek judicial redress to enforce their rights in accordance with the relevant national legislation of the Ibero-American State applicable in this area.

43.2. The relevant national legislation of the Ibero-American States shall establish a framework enabling data subjects to lodge a complaint with the Personal Data Protection Authority where they consider that the processing of their personal data infringes the relevant national legislation, and to seek judicial redress.

43.3. The relevant national legislation of the Ibero-American States shall establish a framework allowing for the adoption of corrective measures and the imposition of sanctions for conduct that contravenes the provisions of the relevant national legislation, specifying, at the very least, the maximum limit and the objective criteria for determining the relevant penalties, based on the nature, seriousness and duration of the infringement and its consequences, as well as the measures implemented by the controller to ensure compliance with its obligations in this regard.

Chapter IX. Right to compensation

44. Complaints procedure and sanctions regime

44.1. The relevant national legislation of the Ibero-American States shall recognise the data subject's right to compensation where they have suffered loss or damage as a result of a breach of their right to personal data protection.

44.2. The domestic law of the Ibero-American States shall specify the competent authority to hear such actions brought by the affected data subject, as well as the time limits, requirements and conditions under which the data subject shall be compensated should the claim be upheld.

Chapter X.

45. Establishment of mechanisms for international cooperation

45.1. Ibero-American States may adopt mechanisms for international co-operation to facilitate the implementation of the relevant national legislation, which may include, by way of example and without limitation:

a. The establishment of mechanisms to strengthen international assistance and co-operation in the implementation of the respective national legislation in this area.

b. Assistance and co-operation between supervisory authorities through the notification and referral of complaints, assistance with investigations and the exchange of information.

c. The adoption of mechanisms aimed at promoting knowledge and the exchange of best practices and experiences in the field of personal data protection, including in relation to conflicts of jurisdiction with third countries.

45.2. Furthermore, as part of international co-operation initiatives, links may be established with networks, forums, mechanisms and other co-operation platforms, which will enable the sharing of regulatory experiences and significant cases, facilitate mutual assistance, develop common positions on disruptive phenomena and emerging issues, promote regulatory interoperability, design common strategies to mitigate regulatory fragmentation, and promote protocols that facilitate administrative simplification, all within the field of personal data protection.

Transitional provisions

Sole provision. To ensure the effective implementation of legislation, regulations and other provisions on personal data protection, including any amendments or reforms, it is essential to provide controllers and processors with the conditions necessary to enable them to comply with such requirements and to ensure that compliance is sustainable over time.

One such condition relates to the timing of regulatory measures, specifically the setting of reasonable timeframes between the publication of the relevant legislation and its entry into force, taking into account the range of material, financial, human resources and regulatory implications that such legislation usually entails.

RED
IBEROAMERICANA DE
PROTECCION
DE DATOS



