RED IBEROAMERICANA DE PROTECCION DE DATOS

Red Iberoamericana
Rede Ibero-Americana

Ibero-American Standards on the Use of Personal Data in Artificial Intelligence Systems

Published in November 2026.



Contents

PREAMBLE

CHAPTER I. GENERAL PROVISIONS, SCOPE AND GENERAL CRITERIA FOR APPLICATION 8

1.1. Purpose 8

1.2. Scope and conditions of application 8

1.3. Processing operations and life cycle 9

1.4. Documentation of processing 9

1.5. Purposes and data reuse 10

1.6. Definitions 10

CHAPTER II. GENERAL DATA PROTECTION PRINCIPLES AND OBLIGATIONS IN PROCESSING OPERATIONS INVOLVING ARTIFICIAL INTELLIGENCE 12

2.1. Lawfulness and legal bases 12

2.2. Fairness, purpose limitation and compatibility 13

2.3. Data minimisation and proportionality 13

2.4. Data quality and accuracy 14

2.5. Transparency and explainability 14

CHAPTER III. SPECIAL CATEGORIES, SENSITIVE INFERENCES AND GROUPS REQUIRING ENHANCED PROTECTION 16

3.1. Inferred sensitivity 16

3.2. People or groups in vulnerable situations 17

3.3. Neurodata 17

CHAPTER IV. AUTOMATED DECISION-MAKING AND PROFILING 18

4.1. Identification of individual automated decisions 18

4.2. Effective human intervention 18

4.3. Effectiveness of safeguards and algorithmic non-discrimination 19

CHAPTER V. INDIVIDUAL RIGHTS IN ARTIFICIAL INTELLIGENCE SYSTEMS 19

CHAPTER VI. STAKEHOLDERS, THE VALUE CHAIN AND INTERNATIONAL TRANSFERS 20

CHAPTER VII. ALGORITHMIC GOVERNANCE, PROACTIVE MEASURES AND IMPACT ASSESSMENT 22

CHAPTER VIII. TECHNICAL AND ORGANISATIONAL MEASURES FOR DATA PROTECTION AND SECURITY IN THE USE OF ARTIFICIAL INTELLIGENCE SYSTEMS 24

8.1. Specific threats and risks 24

8.2. Technical controls and specific tests 24

8.3. Techniques for reducing the risk of identification 25

8.4. Incident response 25

CHAPTER IX. SPECIALISMS APPLICABLE TO SPECIFIC TECHNOLOGICAL AND USAGE PATTERNS 25

9.1. Generative artificial intelligence 25

9.2. Agentic artificial intelligence 26

9.3. Biometrics and emotion recognition 26

9.4. Scoring, selection and prioritisation 27

9.5. Obtaining publicly available data 27

Preamble

Artificial intelligence is profoundly transforming the way in which personal data is collected, used and reused. Its development has increased the ability to draw inferences, automate decisions, reuse information for new purposes and combine large volumes of data in increasingly complex contexts. These developments do not affect the validity of the principles of personal data protection, but they do require clarification as to how they should be applied when processing involves artificial intelligence systems.

To this end, and following a process of drafting, consultation and technical deliberation in which its member authorities have participated, the Ibero-American Data Protection Network hereby adopts these Ibero-American Standards on the use of personal data in artificial intelligence (AI) systems (hereinafter 'the Standard'), designed as a guiding instrument to promote a common understanding of the data protection framework in the context of artificial intelligence within the Ibero-American region and to contribute to the development of artificial intelligence that respects the rights and freedoms of individuals.

The Standard represents a pioneering initiative in systematically developing the specific features introduced by artificial intelligence from the perspective of personal data protection. It does not establish a parallel ethical and legal framework for artificial intelligence, nor does it seek to replace national legislation or the Standards on the Protection of Personal Data for Ibero-American States. Its purpose is to supplement that common framework where the use of artificial intelligence systems raises specific issues that require additional criteria for the application of the principles, rights and obligations relating to data protection, without prejudice to any additional requirements laid down by national legislation. The Standard does not reduce or relax the level of protection recognised by that common framework: the specific provisions it sets out serve as additional criteria for its application, rather than as exceptions to it.

The protection of personal data is a fundamental right of individuals and is based on informational self-determination, understood as the right to decide on the use of one's own personal data and to retain control over its processing; its recognition in the legal systems of the region stems from the need to safeguard human dignity, personal autonomy, equality and other freedoms that may be compromised by the processing of information. The increasing ability to infer, predict and make decisions that characterises artificial intelligence systems makes it particularly important to safeguard that capacity, as processing operations involving such systems may generate data and decisions concerning an individual without their direct involvement and may influence the decisions that affect them. This fundamental right serves as the benchmark against which the provisions of the Standard must be read and interpreted. The Standard neither creates nor supersedes the rights recognised under the general data protection regime and under national legislation: it sets out how those rights are to be exercised when processing involves artificial intelligence systems.

The Standard is based on a pre-existing body of reference legislation, to which it refers using equivalent terms whose scope is defined in the general provisions of the Standard relating to its purpose. The Standard does not seek to replace that body of law or to pre-empt the decisions that fall within the remit of each legal system; its purpose is to clarify how existing obligations and safeguards are to be applied when processing involves the use of artificial intelligence systems. Controllers include public sector

bodies, whose actions are also governed by the provisions of national law relating to the legal basis for processing, the disclosure of data between organisations or to individuals, the publication of information and access to public information, as well as by the duties of transparency imposed on them by that legal framework with regard to the use of artificial intelligence systems. In keeping with its guiding and complementary nature, the Standard is also addressed to these controllers, without prejudice to those rules, which it neither supersedes nor qualifies, and considering the specific characteristics that public action brings to processing operations involving artificial intelligence systems.

The Standard is based on a fundamental principle: its focus is not on artificial intelligence systems viewed in the abstract, but on the processing of personal data that incorporates them. It is from this premise that the life-cycle approach—which forms the backbone of the instrument—derives; the Standard elaborates on this approach by addressing data processing operations and their life cycle, applying the relevant obligations to each processing operation and to the purposes for which it is carried out. In this context, the principle of fairness takes on a particularly important role as a point of reference, as artificial intelligence can widen the gap between the moment when individuals provide their personal data and the way in which that data is subsequently used. The criteria by which fairness is assessed are set out in the Standard, which regulates fairness, purpose limitation and compatibility.

The methodology adopted reflects a deliberate decision to focus on specific regulatory areas: the Standard addresses only those issues where artificial intelligence requires adjustments to the general data protection rules and provides criteria for resolving the specific problems it raises, whilst avoiding unnecessary duplication.

Furthermore, the Standard adopts an approach based on risk and proactive accountability. The measures envisaged must be applied in a proportionate manner, taking into account the nature of the processing, the data used, the purposes pursued, the context of use and the impact that the processing may have on individuals' rights and freedoms. This approach aims to strengthen effective protection without imposing unnecessary burdens or hindering the development and responsible adoption of artificial intelligence.

This approach encompasses assessments of varying nature and intensity: the determination of the legal basis and, where appropriate, the corresponding balancing exercise; the analysis of necessity and proportionality; the identification and assessment of risks to individuals' rights and freedoms and the determination of appropriate measures to manage them; and, where required, the impact assessment. These operations serve their own specific purposes and are complementary to one another: none replaces the others, although the elements documented in one may be used in another where their purpose coincides, and whether each is required is governed by the legal framework applicable to the processing, without the Standard altering when the relevant obligation arises or the conditions to which it is subject. In this context, relying on legitimate interests as a legal basis presents its own difficulties: the scale on which personal data may be reused, the time elapsed between the moment of collection and its subsequent use, and the fact that such processing is often barely noticeable to individuals. These circumstances must be taken into account in the balancing exercise, which must be particularly rigorous where, due to the nature of the data, the scale of the processing, its purposes or its potential effects, there may be greater risks to individuals' rights and freedoms. The calibration of the measures also takes into account the effects of the processing on individuals, for which purpose the Standard deliberately uses two distinct formulations: when it refers to legal effects or a significant impact, it defines the scenario in accordance with the meaning that the general data protection regime attributes to those

terms, without significant impact being limited to consequences of a legal nature, as it also encompasses material, social or economic consequences that the use of artificial intelligence systems is likely to produce; when it refers to effects without qualifying them, it refers to any consequence that processing may have on an individual, without this implying that the intensity of the required measures is standardised; that intensity is determined in accordance with the principle of proportionality to the risks and not by means of a prior classification of the effects.

To this end, the text uses technologically neutral wording — that is, wording that is independent of specific products, brands or suppliers — and avoids imposing specific technical solutions where it is sufficient to define the legal objective to be achieved, without this entailing any dilution of the safeguards afforded to individuals. Its purpose is to provide a stable framework capable of keeping pace with developments in artificial intelligence without creating unnecessary barriers to innovation or losing its usefulness as a reference for data protection authorities, legislators, data controllers and processors, providers of artificial intelligence systems, and other organisations in the public and private sectors.

The Standard shall be interpreted in a manner consistent with the general data protection framework, comprising the Standards on the Protection of Personal Data for the Ibero-American States, together with the other documents and criteria adopted by the Ibero-American Data Protection Network, the applicable national legislation and relevant international instruments. It aims to strengthen regulatory convergence in the region, facilitate the consistent application of data protection in the context of artificial intelligence, and promote a model of responsible innovation that places trust, the protection of individuals and respect for fundamental rights as essential conditions for the development and adoption of artificial intelligence.

Certain applications of artificial intelligence give rise to specific concerns and have been the subject of dedicated studies within the Ibero-American Data Protection Network and by specialised international organisations: the protection of personal data relating to individuals or groups in vulnerable situations, which holds a distinct place within the Ibero-American tradition of data protection; the processing of data relating to neural activity and the drawing of inferences about cognitive, emotional or behavioural states, given their potential to reveal particularly private aspects of a person’s life and their impact on individual autonomy; and the processing of biometric data and the recognition or inference of emotions. The Standard does not replace that body of work or the regime governing these matters under national legislation: it merely sets out the specific issues that arise from the perspective of personal data protection when personal data are processed using artificial intelligence systems. Its criteria on these matters shall be interpreted in line with that work and with developments in the available scientific knowledge regarding the reliability of such systems.

Chapter I. General provisions, scope and general criteria for application

1.1. Purpose

1.1.1. The Standard sets out guiding criteria for the protection of personal data in processing operations that incorporate artificial intelligence systems or are necessary for their development, with the aim of strengthening the protection of individuals and promoting harmonised implementation across the Ibero-American region.

1.1.2. The Standard is intended to provide guidance and is complementary to the general data protection regime. Its provisions apply without prejudice to the provisions of the relevant legal systems and set out how, in accordance with the Standard, data protection obligations and safeguards should be applied where processing involves artificial intelligence systems. The references made in the Standard to the general data protection regime are for explanatory purposes only: they neither condition nor limit the application of that regime, which applies independently of the Standard. For the purposes of the Standard, the terms 'data protection legislation', 'applicable legislation' and 'applicable legal framework' shall be understood to refer to that same general regime; references to specific legislation refer to sector-specific or limited-scope provisions that are additionally applicable under each legal system.

1.1.3. References in the Standard to the general data protection regime shall be understood to refer to the applicable legal system in each case and, as a common reference point for the Ibero-American region, to the Data Protection Standards of the Ibero-American States.

1.2. Scope and conditions of application

1.2.1. The Standard shall apply to the processing of personal data that involves artificial intelligence systems or is necessary for their development, including any inferred or derived personal data generated by such systems, regardless of whether those systems are involved in all or part of the operations constituting the processing. The application of the Standard must be proportionate to the risks arising from the processing, so that it does not impose unnecessary obligations where such risks are limited, nor does it diminish the safeguards required where the processing entails high risks to the rights and freedoms of individuals.

1.2.2. The material, subjective and territorial scopes shall be governed by the general data protection regime, without the Standard affecting the determination of the applicable law under each legal system.

1.2.3. The Standard shall not apply where no personal data are processed, in particular in the case of anonymised data in accordance with the requirements of the Standard, synthetic data that do not allow individuals to be identified or re-identified, or artificial intelligence models that do not process or enable the retrieval of personal data.

1.2.4. Any party invoking the non-application of the Standard must be able to substantiate this, whatever the grounds invoked, and must, for that purpose, have available the analysis on which it is based. If there is subsequently a reasonable risk of identification or re-identification, in accordance with the terms set out in the Standard, the processing shall be subject to its provisions.

1.2.5. Where personal data relating to an identified or identifiable individual can be extracted, disclosed or reasonably attributed to that individual from a model, including its parameters and the results it produces, the processing shall be subject to the Standard.

1.3. Processing operations and life cycle

1.3.1. The application of the Standard will cover the processing of personal data and the purposes for which such processing is carried out and will not extend to artificial intelligence systems or models, nor to the technologies on which they are based, considered in the abstract.

1.3.2. The analysis of processing operations that incorporate artificial intelligence systems or are necessary for their development, regardless of the role the system plays in them, must take into account the various stages of the processing life cycle, in order to identify any changes that may occur in the purposes, the data processed, the parties involved or the risks to individuals, and to determine, in each case, the applicable obligations and safeguards.

1.3.3. For the purposes set out in the preceding paragraph, references in the Standard to development, training, evaluation or improvement denote distinct phases of the processing life cycle. The applicable obligations and safeguards, particularly those relating to lawfulness, data minimisation and data quality, must be determined separately for each phase.

1.4. Documentation of processing

1.4.1. In order to demonstrate compliance with data protection legislation and the Standard, the documentation relating to the processing of personal data must be sufficient, taking into account the nature, complexity and risks of the processing.

1.4.2. Where relevant for the purposes of demonstrating such compliance, the documentation may include decisions taken regarding the design, configuration or use of the artificial intelligence system.

1.4.3. Where processors or providers of artificial intelligence systems or models are involved, the controller must ensure, through the appropriate legal arrangements, that it has the necessary information and documentation regarding the system and, where relevant, regarding any prior processing carried out by the provider, in order to fulfil its obligations, including those relating to transparency and explainability, in accordance with data protection legislation and the Standard. Such information shall include, where necessary, details regarding the source, representativeness and conditions under which the data used were obtained, any known limitations of the system, any identified biases and the mitigation measures adopted. Where personal data provided by the controller or generated or inferred during the provision of the

service are processed beyond the scope of the assignment, compliance with data protection legislation in respect of such data must at least be documented. The conditions governing the use of data by providers during the business relationship are set out in the Standard on Stakeholders, the Value Chain and International Transfers.

1.5. Purposes and data reuse

1.5.1. Where they involve different processing operations or the reuse of data for different purposes, the operational purposes of personal data processing, those relating to development, training, evaluation or improvement, and instrumental purposes – such as security or fraud prevention – must be identified separately.

1.5.2. Where, in the context of processing that incorporates an artificial intelligence system, personal data are used for a purpose other than that for which they were obtained, it must be verified that such use has an appropriate legal basis and, where applicable, the relevant compatibility assessment must be carried out in accordance with the general data protection regime.

1.5.3. The training, fine-tuning or retraining of models shall constitute a separate processing operation where they serve a specific purpose or involve significant changes to the purpose, the data used, the parties involved or the risks associated with the processing.

1.6. Definitions

1.6.1. For the purposes of the Standard as a whole, and without prejudice to the general data protection regime—from which the terms not defined in this section are derived, including those of controller, processor and joint controller, whose identification in processing operations involving artificial intelligence systems is governed by the provisions of the Standard on Stakeholders, the Value Chain and International Transfers—, the following definitions shall apply:

a) Artificial intelligence system: an integrated set of components which, for explicit or implicit objectives and based on input data, generates predictions, inferences, recommendations, content or decisions through machine learning, statistical processing or knowledge-based rules, with varying degrees of autonomy.

b) Model: an artefact resulting from training or fine-tuning which incorporates, within its parameters, patterns derived from the data used and which, when applied to new data, produces inferences or predictions. The defining feature of an artificial intelligence system is the inclusion of one or more models.

c) Inference: a result that the system derives, predicts or estimates from input data, including attributes, behaviours, preferences or categories not provided by the data subject.

d) Training and fine-tuning: operations that build or modify a model so that it fulfils predefined purposes to an adequate level of quality; these include initial training and subsequent fine-tuning or specialisation operations.

e) Development: preparatory activities for training, including system design, architecture selection, preparation and exploration of datasets, and experimental testing, which do not in themselves constitute training or fine-tuning.

f) Inferred and derived data: personal data generated by the system. Inferred data result from a prediction, estimate or hypothesis; derived data result from the transformation or combination of pre-existing data.

g) Synthetic data: data generated artificially to replicate the statistical properties of a reference set, without corresponding to specific individuals. The fact that data are synthetic does not in itself imply that any reference data, if any, have been anonymised.

h) Artificial intelligence provider: a person who develops, trains, supplies or operates artificial intelligence models or services for incorporation by others into personal data processing operations.

i) Neurodata: personal data obtained through specific technical processing (whether directly, indirectly or by inference), relating to the anatomical, physiological, functional or behavioural characteristics of a natural person in connection with the activity of their brain and nervous system.

j) Vulnerable individuals or groups: those who, whether permanently or temporarily, and by reason of their age, disability or other personal, social, economic or contextual circumstances, including those specific to the digital environment, are at greater risk of harm or face greater difficulties in understanding, controlling or exercising their rights in relation to the processing of personal data or the use of artificial intelligence systems.

Chapter II. General data protection principles and obligations in processing operations involving artificial intelligence

2.1. Lawfulness and legal bases

2.1.1. The lawfulness of processing and the legal bases on which it may be founded are governed by the general data protection regime, which sets out the permissible legal bases and the conditions for their use; this paragraph neither lists nor ranks them, but merely specifies their application where processing involves artificial intelligence systems.

Whether a new legal basis or a compatibility assessment is required will depend on whether the purpose of the processing or the conditions that initially justified its lawfulness have changed. Consequently, the various stages of an artificial intelligence system's life cycle do not, in themselves, constitute separate processing operations, nor do they necessarily require a separate legal basis.

2.1.2. Where permitted by the applicable legal system, and subject to the conditions laid down therein, legitimate interests may constitute an appropriate legal basis for certain processing operations carried out for the purposes of developing, training, evaluating or improving artificial intelligence systems, provided that a proper balancing exercise is carried out and the necessary technical and organisational measures are taken to protect the rights and freedoms of individuals. The suitability of a legitimate interest as a legal basis may not be presumed. In carrying out this balancing exercise, the following factors, amongst others, may be particularly relevant: the nature of the data being processed and the context of the processing; the application of data minimisation or pseudonymisation measures; the reasonable expectations of individuals regarding such use, the impact on them and the severity of the risks to their rights and freedoms, the absence of decisions having legal effects or significantly affecting individuals in a similar manner during those stages, and the possibility of effectively exercising the right to object. The existence of this legal basis does not exempt controllers from the principles of purpose limitation and data minimisation, nor from the techniques for reducing the risk of identification set out in the Standard, which apply to each of the stated purposes.

The balancing exercise must be particularly rigorous where the processing involves the large-scale reuse of personal data, special categories of data, data relating to individuals or groups in a vulnerable situation, or profiling activities that may produce legal effects or otherwise significantly affect individuals in a similar way. Such a balancing exercise does not exempt the processing of special categories of data from the specific regime applicable to them, whose conditions of lawfulness and enhanced safeguards must also be met; nor does it replace the impact assessment, nor is it replaced by it, as these are distinct requirements.

2.1.3. In the case of processing carried out by public sector bodies in the exercise of public functions or powers of authority, the admissibility of the legitimate interest and the determination of the legal bases on which the processing may be founded are governed by the legal basis requirements laid down by the applicable legal system.

2.2. Fairness, purpose limitation and compatibility

2.2.1. The principle of fairness is particularly important in the processing of personal data for the purposes of developing, training, evaluating or improving artificial intelligence systems, as well as in processing operations that generate profiles, classifications or prioritisations of individuals, or make decisions about them based on such operations, particularly where this involves reusing personal data for purposes other than those for which they were obtained. In such cases, the assessment of fairness will be based on whether the actual processing of data corresponds to what individuals can reasonably expect when they provide their personal data.

2.2.2. The use, by providers or processors, of personal data processed on behalf of the controller for their own purposes, such as the development, training, evaluation or improvement of artificial intelligence models or services, shall generally be considered a separate purpose and shall not be deemed to be included within the scope of the processing entrusted to them, unless there is express legal authorisation and a legal basis to support it. For these purposes, the anonymisation or transformation of such data carried out for those specific purposes constitutes a use subject to the provisions of this paragraph; the anonymised result cannot be regarded as covered by the processing arrangement if the operation that produced it was not.

2.2.3. The fact that personal data or public data is accessible to the public does not justify its use for the development, training or improvement of artificial intelligence models or systems.

2.2.4. Processing operations involving artificial intelligence systems designed to misleadingly manipulate people's behaviour or to unduly exploit situations of vulnerability — including those arising from age, disability or socio-economic status — or to establish social scoring mechanisms that result in discriminatory effects or unjustified restrictions on rights are incompatible with the principles of data protection. The provisions of this paragraph are without prejudice to the enhanced safeguards laid down in the Standard for processing operations involving biometric techniques and for the collection of personal data accessible to the public, applicable to the creation or expansion of biometric databases through mass, systematic and indiscriminate collection of images or recordings, as well as the prohibitions, limitations or additional requirements laid down by the applicable regulations.

2.3. Data minimisation and proportionality

2.3.1. In the context of data processing involving artificial intelligence, the principle of data minimisation also applies to the system's ability to identify, single out or draw inferences about individuals, and such outcomes must be avoided where they are not necessary for the purpose of the processing.

2.3.2. Data minimisation must take particular account of data selection and the drawing of inferences during processing.

2.3.3. In processing operations that use artificial intelligence systems to identify or verify a person's identity, a clear distinction must be made between identification and identity verification, considering their different risks and safeguards. This distinction does not prejudge the lawfulness of such processing, which shall be determined in accordance with the general data protection

regime and the specific applicable regulations, nor does it preclude the classification of the data used as special categories where appropriate under that regime, with the enhanced safeguards that this entails.

2.4. Data quality and accuracy

2.4.1. The quality and accuracy of data processed using artificial intelligence systems, as well as the inferences and results obtained from such processing, must be assessed in terms of their suitability for the purpose of the personal data processing and the context of use. Accuracy requires the degree of conformity with reality necessary to fulfil that purpose and protect people's rights, without absolute correspondence being required in every case. Where the data, inferences or results are to serve as the basis for decisions that have legal effects on a person or significantly affect them in a similar manner, the requirement for accuracy and up-to-date information shall be assessed with particular rigour, without prejudice to the rights to rectification, updating and erasure recognised by the general data protection regime and their implications for inferences, results and models previously trained in accordance with the provisions of the Standard on the rights of individuals.

2.4.2. Where inferences or findings may have an impact on an individual, they must be used with due regard to their nature as hypotheses, deductions or proposals and the degree of uncertainty associated with them; they must not be treated as established facts where there is insufficient basis for doing so, and must not be presented as such to the individual or to third parties. In accordance with the risk-proportionate application rule set out in the Standard regarding scope and conditions of application, the level of rigour required in that assessment shall be determined in accordance with the significance of the effects that the inferences or results may have on the individual. The nature of the inference or the result does not affect the safeguards applicable to the personal data used to generate them.

2.4.3. The required quality and accuracy may vary depending on the purpose and stage of the processing. In the development, training, validation or testing of artificial intelligence systems, provided that it is appropriate for the purpose of those activities and does not have any undue effects on individuals or their rights, data may be used that does not meet the same requirements as those applicable during the system's operational phase. This provision relates to the required standards of quality and accuracy and does not, in itself, presuppose or authorise the use of personal data in such activities, to which the principles of lawfulness, purpose limitation and data minimisation, as well as the techniques for reducing the risk of identification set out in the Standard, are equally applicable.

2.5. Transparency and explainability

2.5.1. Where the processing of personal data involves the use of an artificial intelligence system, the controller must inform data subjects, in terms that are easy to understand in accordance with this paragraph, of the use of the system, the purpose for which it is used, the role it plays in the

processing, and the consequences it may have for them. Merely stating that artificial intelligence or algorithms are used does not fulfil the duty to provide information.

2.5.2. The information will enable data subjects to understand the categories and sources of the data; whether the system generates profiles, inferences, classifications, recommendations or decisions; the recipients and, where relevant, the involvement of suppliers or third parties; the retention criteria and, where specified, the applicable time limits; the extent of human intervention; the reasonably foreseeable consequences; and the means of exercising rights and lodging appeals. The description of human intervention shall set out its actual role and shall not present merely formal supervision as a guarantee.

2.5.3. Where necessary to understand the processing or to exercise their rights, the individual will be provided with a meaningful explanation in language they can understand. The explanation will cover the logic of the system, the factors that have a significant influence on the result, the relevant data sources, known limitations, and measures for detecting and correcting errors and biases. There is no obligation to disclose the source code, the complete model or any information whose disclosure would compromise security, trade secrets or intellectual property, provided that the person retains a sufficient understanding of the processing. This restriction applies solely to the content of the explanation required and does not exempt the party from providing any additional information necessary to ensure such sufficient understanding, without prejudice to the provisions of this paragraph concerning the essential content of the right to information. Nor does it affect the supervisory powers conferred on data protection authorities by the applicable legislation, nor the additional requirements laid down by the specific legislation applicable to transparency and access to public information. The explanation may also be supported by the results of audits, certifications or trust seal schemes that provide assurances regarding the functioning of the system; however, this shall not replace the required explanation or reduce its scope.

2.5.4. The scope and level of detail of the information and explanation shall be determined by the impact of the processing of personal data, the degree of automation and the complexity of the system. In the case of an automated individual decision, the information and explanation will help the individual understand the safeguards in place and the avenues available to them for requesting human intervention, challenging the decision or exercising their rights.

2.5.5. The information may be presented in layers or levels of detail, provided that this enables individuals to understand the processing and to effectively exercise their rights. The protection of security, trade secrets or intellectual property may not be invoked to undermine the essential substance of the right to information or to prevent the effective exercise of the rights recognised to individuals under the general data protection regime.

Chapter III. Special categories, sensitive inferences and groups requiring enhanced protection

3.1. Inferred sensitivity

3.1.1. Health, ideology, sexual orientation or beliefs can be inferred even from seemingly neutral variables. Other particularly sensitive inferences may also be drawn, including those relating to economic vulnerability. Where such inferences do not in themselves constitute special categories of data, they must be assessed in light of their effects on individuals, in accordance with the principle of proportionality to the risks and the impact assessment provided for in the Standard, subject to the terms and conditions set out therein. The enhanced regime provided for by the general data protection regime in respect of special categories of data shall be determined by the actual nature of the information inferred, and not solely by that of the input data.

3.1.2. The enhanced regime provided for in the general data protection regime in respect of special categories of data shall apply where the system generates or uses inferences that make it possible to reasonably attribute a special category of data to an individual. The purpose, context and impact of the processing will be taken into account when assessing the reasonableness of such an attribution. The degree of reliability or accuracy of the inference shall not, in itself, preclude the application of the enhanced regime where that inference is used to make or support decisions concerning the individual.

3.1.3. The incidental presence of special categories of data during the development or training of a system must be assessed separately for each of these phases, in accordance with the life-cycle approach generally set out in the Standard, taking into account whether such data are used, may influence the model, or may be disclosed through its inferences or results. The controller shall take reasonable steps to limit the use of such data and to prevent them from being used as a basis for drawing conclusions or making decisions about individuals where this is neither necessary nor lawful.

3.1.4. The processing of special categories of data, or of inferences that make it possible to reasonably attribute such categories, including their storage and use, may only take place where one of the exceptions provided for by the general data protection regime in respect of those categories applies. The Standard does not in itself constitute authorisation for such processing. Where the general data protection regime permits it for the purpose of detecting, assessing or rectifying discriminatory effects or biases, the processing shall be subject to the principles of data minimisation and proportionality and to the enhanced safeguards required under the Standard and that regime.

3.2. People or groups in vulnerable situations

3.2.1. In the case of artificial intelligence processing that affects individuals or groups in vulnerable situations, their best interests must be considered both in determining the processing and in the assessment and use of the inferences and results generated by the system.

3.2.2. The use of personal data relating to individuals or groups in vulnerable situations for the development, training, validation or improvement of artificial intelligence systems shall, at each of these stages, require particularly rigorous justification and the adoption of enhanced safeguards, taking into account their best interests. The scope of these safeguards will be determined in light of the risks associated with the processing of this group's data and the requirements laid down by the general data protection regime in respect of their personal data. Where such processing is not necessary for the intended purpose, measures must be taken to prevent the use of these data.

3.2.3. In systems aimed at individuals or groups in vulnerable situations, or which may significantly affect them – including cases involving discriminatory effects – particularly protective and pre-set configurations must be applied, along with age-appropriate design and enhanced safeguards against profiling, behavioural advertising and the improper collection of their personal data, in accordance with the principles of data protection by design and by default set out in the Standard. These measures do not, in themselves, authorise the processing of personal data; the lawfulness of such processing is governed by the general data protection regime and by the prohibitions and restrictions laid down therein. Profiling, behavioural advertising and inferences that unduly exploit the vulnerable situation of these individuals or groups are deemed to be incompatible with the data protection principles set out in general terms by the Standard. Where, despite the measures taken, a high risk to this group persists, the general provisions set out in the Standard shall apply in cases where the high risk persists. The information and explanation required under the Standard shall be provided in terms that are understandable, taking into account their age.

3.3. Neurodata

3.3.1. The controller shall subject processing operations carried out using artificial intelligence systems that utilise neurodata or generate inferences regarding cognitive, emotional or behavioural states to a specific assessment of necessity and proportionality, taking into account their capacity to reveal particularly sensitive aspects of the individual, the context in which they are carried out – particularly where relationships characterised by a power imbalance are involved – and the risks they may pose to autonomy, privacy and fundamental rights. This assessment is without prejudice to any impact assessment that may be required under the applicable regulations and the Standard.

3.3.2. Processing operations that use neurodata or inferences about cognitive, emotional or behavioural states to unduly manipulate individuals' will or behaviour, or to exploit situations of vulnerability, are incompatible with the principles of data protection, as set out in general terms by the Standard. Processing aimed at inferring deeply held convictions or carrying out particularly intrusive forms of surveillance may only be permitted in exceptional circumstances

where there is an admissible legal basis under the general data protection regime, the processing serves a particularly relevant legitimate purpose (the particular relevance of which must be justified), is necessary and proportionate, and no less intrusive alternatives exist, without prejudice to any prohibitions, limitations or additional requirements laid down in the applicable specific legislation. It must be possible to demonstrate that all these conditions are met, in accordance with the duty to document processing set out in the Standard. Consent should not constitute a lawful basis where the controller is unable to determine in advance, with reasonable accuracy, what inferences will be drawn from the processing of neurodata.

Chapter IV. Automated decision-making and profiling

4.1. Identification of individual automated decisions

4.1.1. The controller shall identify the cases in which a decision is based solely on automated processing, including profiling, which produces legal effects concerning the data subject or significantly affects them, whatever the nature — social, economic or otherwise — of that impact, distinguishing between fully automated decisions, decision-support systems and cases of effective human intervention in accordance with the criteria set out in this chapter. The identification of these cases will determine the application of the duties of transparency and explanation, and of the safeguards provided for in the Standard in relation to automated individual decisions.

4.1.2. This assessment will be reviewed whenever there are significant changes to the processing or to the artificial intelligence system, in order to determine and adapt the applicable safeguards, taking into account, amongst other factors, the significance of the effects of the processing, the stage of the processing life cycle and the characteristics of the system.

4.2. Effective human intervention

4.2.1. The exclusively automated nature of a decision shall only be excluded where there is prior, genuine and effective human intervention by a person capable of assessing and understanding the system's output and with sufficient authority to confirm, amend or override it. Human intervention shall not be deemed to be effective if it is limited to formalising or endorsing the system's outcome without meeting those conditions; in such a case, the decision shall retain its exclusively automated nature and shall be subject to the safeguards against individual decisions set out in this chapter, as well as the duties of information and explanation laid down in the Standard on transparency and explainability. The organisational conditions necessary for such intervention to be effective – including the allocation of responsibilities, training and supervision of those carrying it out – shall be adopted in accordance with the algorithmic governance measures set out in the Standard.

4.2.2. Human supervision may be supported by automated tools, such as alert systems or discrepancy detection systems; however, these will not replace human intervention where this is required, nor may they be presented as equivalent to it. The use of such tools will not alter the conditions set out in this chapter whereby human intervention precludes the decision from being made exclusively by automated means.

4.3. Effectiveness of safeguards and algorithmic non-discrimination

4.3.1. The safeguards applicable to individual decisions include, at a minimum and in accordance with the terms set out in the Standard: information on the use of the artificial intelligence system, the purpose for which it is used, the role it plays in the processing and the consequences it may produce, as well as a meaningful explanation of the processing, in accordance with the provisions of the Standard regarding transparency and explainability; information on the available channels for requesting human intervention, challenging the decision and exercising the relevant rights; and the measures for the prevention, detection and correction of discriminatory effects set out in this chapter. These safeguards shall be accessible, timely and effective in practice, rather than merely formal, enabling individuals to understand the decision and its consequences, to request human intervention where appropriate, and to exercise the rights granted to them under data protection legislation.

4.3.2. The controller shall assess whether the system is capable of producing discriminatory effects, including those arising from the use of apparently neutral variables, from significant differences in its operation in relation to different groups of people, or from the inferences generated by the system, and shall take the necessary measures to prevent, detect and correct any biases that may unjustifiably affect individuals. The appropriateness and adequacy of these measures must be capable of being demonstrated in accordance with the duty to document the processing set out in the Standard, without prejudice to the powers vested in data protection authorities under the applicable legislation.

Chapter V. Individual rights in artificial intelligence systems

5.1. The rights recognised under data protection legislation may be exercised in respect of personal data processed using artificial intelligence systems, including inferences, profiles and other outputs that constitute personal data. The nature of this data may determine the scope or manner in which each right is exercised, without prejudice to the provisions of the aforementioned regulations.

5.2. When exercising their right of access, individuals may find out, where applicable in accordance with data protection legislation, whether their data have been used in an artificial intelligence system, whether profiles or inferences have been generated about them, and whether these have influenced or been used to make or support decisions affecting them.

5.3. Where the right to rectification relates to inferences, profiles or predictions generated by an artificial intelligence system, the manner in which it is exercised must be adapted to their nature. Where such data cannot be rectified directly due to their very nature, the individual may request

the correction of the data used to generate them, provide additional information, contest them or request their review, particularly where they may have an impact on them.

5.4. The exercise of the rights to erasure, restriction and objection shall be governed by the general data protection regime. The controller shall endeavour to select, configure or use systems that incorporate, provided that this is technically feasible given the state of technology and the resources reasonably available, mechanisms that facilitate the effective exercise of these rights throughout the entire processing life cycle, in particular by deleting, unlinking or excluding personal data from future training processes. The technical feasibility of such mechanisms does not affect the enforceability of these rights, and the assessment of such feasibility must be documented in accordance with the duty to document processing set out in the Standard, without prejudice to the powers vested in data protection authorities under the applicable legislation.

5.5. Where, due to the state of technology, the rights to erasure, restriction or objection cannot be fully exercised in respect of a pre-trained model, the controller must justify this circumstance and record it in accordance with the duty to document the processing set out in the Standard, inform the data subject thereof, and take all reasonably available measures to restrict the processing and minimise its impact, including, where possible, the erasure of personal data from the environments in which they are held — including, amongst others, training datasets, indexes, vector representation databases and persistent storage — and their exclusion from future training. This circumstance shall not be definitive and shall be assessed in accordance with the state of technology at any given time. The provisions of this section are without prejudice to the duty of the controller, when using artificial intelligence models or services developed by third parties, to verify the conditions of their use in accordance with the provisions of the Standard relating to actors and the value chain, and to the liability incumbent upon each party involved in accordance with that regime.

5.6. Data portability applies to the data provided by the data subject and, where applicable, to any observed data that are in a structured format. Under the general data protection regime, data portability shall not, as a general rule, include inferred or derived data, without this affecting their status as personal data or the data subject's exercise of the other rights recognised in respect of such data. Structured formats may be provided to facilitate interoperability and the ability to switch providers.

Chapter VI. Stakeholders, the value chain and international transfers

6.1. The status of controller or processor – and, where the applicable legal framework recognises this role, that of joint controller – shall be determined in relation to each instance of personal data processing; the controller is the party that determines the purposes and the essential means of the specific processing, even if it does not train or technically control the model. Where several parties share such decisions, the responsibilities assumed by each must be determined at the

data processing design stage, defined in accordance with the provisions of the Standard on the relationships between the parties involved in the processing, and documented in accordance with the duty to document the processing set out in the Standard.

6.2. Providers of models or artificial intelligence services may act as controllers, processors or joint controllers, depending on the functions they perform in each processing operation, assessed in accordance with the processing lifecycle and considering decisions taken in earlier stages that have a significant impact on it. In particular, when they reuse personal data for their own purposes or determine the purposes or the essential means of processing, they shall assume the relevant responsibilities in accordance with data protection legislation. The conditions governing the use of data for the development, training or improvement of models must be expressly determined between the parties; however, such determination shall not replace the legal basis required for the processing, nor the provisions of the Standard regarding fairness, purpose limitation and compatibility in relation to the use of personal data by providers or processors for their own purposes.

6.3. The controller shall identify the parties involved in the development, provision and use of the artificial intelligence system, including processors, sub-processors and successive suppliers involved in the processing, as well as the processing operations or functions carried out by each party in relation to personal data and any international transfers that may take place. This identification should make it possible to determine the responsibilities of each party involved, formalise the relevant legal relationships and provide the information necessary to comply with data protection regulations. The foregoing is without prejudice to the information that must be provided to individuals regarding the recipients and the involvement of suppliers or third parties, which shall be governed by the provisions of the Standard relating to transparency and explainability.

6.4. The use of artificial intelligence models or services developed by third parties does not exempt the controller from verifying that their use is compatible with data protection legislation, nor from assessing the safeguards offered by those providers, particularly where the characteristics of the model or the terms and conditions of the service may affect the processing of personal data. The selection of suppliers must take into account, amongst other factors, the nature of the data being processed and the purposes of the processing, the safeguards they provide to ensure compliance with data protection regulations and the information they make available to the controller to demonstrate such compliance, including information relating to the parties involved in the provision of the service, any restrictions that may affect the processing, and the mechanisms in place to notify the controller of any relevant changes to the service provision. The provisions of this section are without prejudice to the information and documentation which the controller must hold regarding the system and the prior processing operations carried out by the provider, in accordance with the duty to document the processing set out in the Standard.

6.5. The relationships between the various parties involved in data processing, including sub-processors and subsequent service providers, must clearly define the responsibilities assumed by each party, in particular with regard to the use of personal data, including the application of anonymisation techniques to such data, their use for the development, training or improvement of models in accordance with the provisions of the Standard on fairness, purpose limitation and compatibility, the exercise of individuals' rights, international transfers and those obligations whose fulfilment depends on the actions, capabilities or resources available to the provider.

6.6. International transfers of personal data carried out in the context of the development, training, deployment or use of artificial intelligence systems shall be subject to the general data protection regime. Where the context of the processing or the risks associated with the use of artificial intelligence systems so require, appropriate additional measures must be taken in respect of the data being transferred, such as data minimisation, encryption, pseudonymisation or additional contractual safeguards regarding their use, retention or reuse. The identification of any transfers that may take place where suppliers or sub-processors are involved shall be governed by the provisions of this chapter on the identification of the parties involved in the processing.

Chapter VII. Algorithmic governance, proactive measures and impact assessment

7.1. Data protection by design and by default must be applied and integrated into the governance of processing throughout the entire life cycle of processing operations involving artificial intelligence systems, taking into account the specific risks arising from their development, training, deployment, use and evolution, and applying the principle of data minimisation to each of these phases in accordance with the terms set out in the Standard.

7.2. The documentation and record-keeping of processing activities shall, in respect of processing operations involving artificial intelligence systems, fulfil the evidential function associated with the duty to document processing as set out in the Standard, and shall identify, where relevant, the specific features arising from the use of such systems. These specific characteristics shall include the categories and origin of the input data, the attributes, profiles, inferences or classifications that the system generates or could reasonably generate, and the categories of results it produces, as well as the intended purposes and uses of such results.

7.3. The controller shall put in place appropriate, risk-proportionate and verifiable algorithmic governance measures to ensure compliance with data protection regulations throughout the entire processing life cycle. These measures shall include, where appropriate, the allocation of responsibilities, risk management, human oversight, appropriate training for those involved in the processing and, in particular, in the configuration, use or monitoring of the artificial intelligence system, coordination between the relevant functions within the organisation, and the periodic review and continuous improvement of the measures adopted. The appropriateness of these measures shall be assessed in the light of the nature, context, scope and purposes of the processing, and the risks it may pose to individuals' rights and freedoms, without prejudice to the powers vested in data protection authorities under the applicable legislation.

7.4. Where it is necessary to appoint a data protection officer in accordance with the applicable legislation, that person shall be involved from the initial stages of any processing operations involving artificial intelligence systems, with access to the necessary information, training and resources to carry out their duties effectively and not merely as a formality.

Where the organisation has specific functions or bodies responsible for the governance of artificial intelligence, these shall coordinate their actions with the data protection officer on

matters relating to the processing of personal data, whilst respecting the functional autonomy of each.

7.5. Where required by the applicable regulations, the controller must carry out an impact assessment prior to the commencement of processing and its deployment, and review it whenever there are significant changes to the data, the purposes, the artificial intelligence models and systems used, the suppliers or the risks to individuals. It is recommended that this be carried out, irrespective of whether it is required by law, where the processing may pose a high risk to individuals' rights and freedoms. The assessment shall pay particular attention to the risks arising from the use of automated decision-making, profiling and any potential discriminatory or adverse effects on the individuals or groups concerned, where these are relevant to the processing; where the processing is likely to produce such effects or affect individuals or groups requiring enhanced protection, efforts shall be made to seek the views of the individuals or groups potentially affected or their representatives. The scope and level of documentation of the assessment must be proportionate to the nature, context and risks of the processing.

7.6. Where the assessment identifies high risks, the controller must take additional measures to mitigate them. If, despite this, a high risk persists, the controller must consult the relevant data protection authority before commencing the processing or deploying the system, or refrain from commencing the processing. Where the applicable regulations provide for a specific procedure in such cases, that procedure shall be followed. Particular care must be taken in the identification, assessment and management of risk, amongst other things, in relation to processing operations involving automated decisions that produce legal effects on individuals or significantly affect them, social scoring or the generalised assessment of individuals, biometric identification or the recognition or inference of emotions, remote biometric identification in public spaces, the processing of neurodata or the generation of inferences regarding cognitive, emotional or behavioural states, the processing of data relating to individuals or groups in vulnerable situations, or the mass reuse of personal data for the development or training of artificial intelligence systems, all in accordance with the provisions of the Standard regarding groups subject to enhanced protection, neurodata, and technological and usage patterns, and without prejudice to any processing that the Standard declares to be incompatible with the principles of data protection.

7.7. Compliance with codes of conduct, technical standards or certification schemes, as well as the assessment, authorisation, certification or supervision of an artificial intelligence system in accordance with the specific regulations applicable to it, may facilitate the application of the Standard and demonstrate the adoption of good practices, but they do not replace the responsibility of the controller to ensure compliance with data protection legislation or the proper management of risks arising from the use of artificial intelligence systems, and are without prejudice to the powers of the data protection authorities under the applicable legal framework.

7.8. In the case of processing operations involving high risks, the periodic review and continuous improvement of the algorithmic governance measures set out in this chapter shall be stepped up in line with the significance of those risks, and it is also recommended that independent reviews or audits be carried out where these help to verify the effectiveness of the measures adopted, strengthen algorithmic governance and improve risk management. When such

assessments are carried out, care shall be taken to ensure that they are based on predefined evaluation criteria commensurate with the risk involved, and that the independence, technical competence and absence of conflicts of interest of those carrying them out can be verified

7.9. Any documentation produced on the basis of these Standards must be made available to the competent data protection authority in the performance of its supervisory functions, in accordance with paragraph 42.4 of the Data Protection Standards of the Ibero-American States.

Chapter VIII. Technical and organisational measures for data protection and security in the use of artificial intelligence systems

8.1. Specific threats and risks

The controller shall identify and keep up to date a list of specific artificial intelligence threats applicable to their system, including, amongst others, the extraction of training data, model inversion, membership attacks, leaks via system instructions, exposure of vector representations, re-identification, memorisation, training data poisoning, unauthorised retrieval of information in retrieval-augmented generation systems, and instruction injection.

Identifying these threats and assessing the risk they pose to individuals' rights and freedoms will serve as the basis for defining the appropriate security measures, testing procedures and incident response procedures to protect the personal data being processed. Where the processing involves combining different sources of information, the risk of aggregation and re-identification must be assessed.

8.2. Technical controls and specific tests

Security measures must be maintained and reviewed throughout the entire lifecycle of personal data processing. The controller shall implement appropriate legal, technical and organisational measures to address the identified threats and the specific risks they pose to the processing of personal data. These may include, amongst others, access controls, environment segregation, encryption, monitoring, isolation of environments or components, mechanisms for filtering and validating inputs and outputs, measures to limit the memorisation or disclosure of personal data, and other technical and organisational measures adapted to the state of the art, the evolution of threats and the risk associated with the processing. It shall also carry out appropriate tests to verify the effectiveness of these measures as part of its review and whenever there are significant changes to the processing or to the artificial intelligence system. To this end, it may rely on generally recognised technical standards, methodologies or guidelines, provided that these are appropriate to the risks associated with the processing and contribute to the continuous improvement of the controls put in place, without prejudice to the value that the Standard attaches to codes of conduct, technical standards and certification schemes.

8.3. Techniques for reducing the risk of identification

8.3.1. Pseudonymisation reduces exposure, but does not remove the processing from the scope of the general data protection regime. Anonymisation may only be considered effective where it is established that there is no reasonable risk of identification or re-identification, taking into account the means that may reasonably be used; this assessment requires particular caution where the processing, the system or its results may facilitate re-identification or reveal data through memorisation. These techniques constitute data protection by design and by default measures, in accordance with the terms set out in the Standard.

8.3.2. Depending on the circumstances, techniques such as pre-filtering of data, removal of duplicates, reduction of the level of detail in the information, pseudonymisation, differential privacy, synthetic data or other measures designed to reduce the risk of identification may be used. The use of these techniques does not dispense with compliance with data protection regulations or the adoption of appropriate security measures.

8.4. Incident response

8.4.1. The controller shall take into account, in its incident management procedures, the specific vulnerabilities arising from the use of artificial intelligence systems, in particular those that may lead to the disclosure, extraction or misuse of personal data or to a loss of availability, and shall incorporate these vulnerabilities into the general incident management procedures. It shall also provide for appropriate measures for their detection, containment and mitigation, as well as for the assessment of the risk to individuals' rights and freedoms. Where applicable, the response to the incident shall comply with the general data protection regime applicable to personal data breaches, including the notification required under that regime to the competent data protection authority and, where appropriate, to the data subjects.

Chapter IX. Specialisms applicable to specific technological and usage patterns

In addition to the general provisions contained in the Standard, where a processing operation incorporates any of the following technological or usage patterns, the specific provisions set out in this chapter shall apply, to the extent that they are relevant.

9.1. Generative artificial intelligence

In processing operations that incorporate generative artificial intelligence systems, specific measures must be taken to prevent the unnecessary inclusion of personal data, whether the organisation's own or that of third parties, in the instructions; define the conditions for the retention of the instructions and outputs, as well as their possible use for training or improving models; prevent the unauthorised

disclosure, retrieval or memorisation of personal data; and verify the results where they may be used to make decisions affecting individuals. This verification is without prejudice to the accuracy required of the inferences and results in accordance with the Standard. Where the processing involves the development or training of models, sufficient information must be available regarding the origin of the data used, in accordance with the duty to document the processing set out in the Standard.

9.2. Agentic artificial intelligence

Where an artificial intelligence system is able to access personal data autonomously or carry out actions on such data, the controller must determine the permissible level of autonomy, taking into account the actions the system may carry out and their potential effects on individuals, such that the greater the significance of those effects, the lower the degree of autonomy and the more intensive the supervision; define the data, tools, services or resources to which the system may have access; control the use of persistent memory where this involves the retention or reuse of personal data, which shall be subject to the principles of purpose limitation and storage limitation in accordance with the Standard and data protection regulations; ensure the traceability of actions, including access to authorised resources and interactions with other systems, services or agents; and provide for mechanisms for human oversight and for the suspension or interruption of actions, which must be capable of being activated independently of the system itself, where necessary to protect individuals' rights. The system's autonomous actions must remain within the scope of the processing and the purposes previously determined by the controller. Where the system's autonomous processing serves a purpose other than that originally intended, it must be verified that there is an appropriate legal basis for such processing and, where applicable, that it is compatible with the original purpose, in accordance with the provisions of the Standard on purposes and the reuse of data. The fact that the system operates autonomously does not exempt or override the responsibilities incumbent upon those involved in data processing in accordance with the Standard and data protection legislation.

9.3. Biometrics and emotion recognition

Processing operations that incorporate artificial intelligence systems and biometric techniques – regardless of whether these are used by the system itself – must distinguish, amongst other cases, verification, identification and other uses of biometric techniques, in accordance with the distinction between identification and verification of identity set out in the Standard on minimisation and proportionality, applying, where appropriate, the enhanced safeguards required under data protection legislation, including those arising from the enhanced regime for special categories of data set out in the Standard on inferred sensitivity where applicable, and taking into account the risk associated with the processing. Remote biometric identification and, where they involve the processing of personal data, the recognition or inference of emotions and other uses which, by virtue of their nature, context or scope, may significantly affect individuals' rights, shall require particularly rigorous attention, without prejudice to the prohibitions, limitations or additional requirements laid down by the applicable specific regulations and to the provisions of the Standard for processing operations that generate inferences regarding cognitive, emotional or behavioural states. In such cases, it must be possible to demonstrate – in accordance with the requirements regarding quality, accuracy and documentation of processing set

out in the Standard – that the system is suitable and reliable for the purpose and context in which it is used. These processing operations are also included amongst those requiring particularly rigorous attention in terms of risk identification, assessment and management, and amongst those that necessitate more frequent periodic reviews and the continuous improvement of algorithmic governance measures, in accordance with the terms and conditions set out in the Standard.

9.4. Scoring, selection and prioritisation

Processing operations that incorporate artificial intelligence systems designed to evaluate, select, classify or prioritise individuals must include specific measures to prevent discriminatory outcomes, in accordance with the provisions of the Standard on the effectiveness of safeguards and algorithmic non-discrimination, ensure a level of transparency commensurate with their impact, in accordance with the provisions of the Standard on transparency and explainability, and ensure compliance with the safeguards applicable to automated individual decisions where appropriate, without prejudice to the prohibitions, limitations or additional requirements laid down by the specific applicable legislation and to the general incompatibility established in the Standard for social scoring mechanisms that produce discriminatory effects or unjustified restrictions on rights.

9.5. Obtaining publicly available data

The use of publicly available personal data for the development, training or improvement of artificial intelligence models or systems is governed by the rule set out in the Standard regarding fairness, purpose limitation and compatibility, according to which the fact that the data are publicly available does not, in itself, legitimise such use. Their public availability does not preclude the application of the principle of purpose limitation either. The reuse of such data for purposes other than those that justified their publication or collection will require an appropriate legal basis and, where appropriate, enhanced safeguards, without prejudice to the compatibility assessment required under the provisions of the Standard relating to purpose limitation and data reuse. These safeguards will be particularly necessary where reuse takes place through large-scale compilations or is based on a legitimate interest, in legal systems that recognise this legal basis, without the public accessibility of the data in itself constituting such a legitimate interest or exempting the controller from the balancing exercise required under the Standard In determining the appropriate legal basis and the relevant safeguards, account shall be taken of the purpose and context that justified the data being made available to the public, as well as the reasonable expectations of individuals regarding such reuse. Such safeguards may include the techniques for reducing the risk of identification set out in the Standard, applied with particular attention to special categories of data and to data relating to individuals or groups in vulnerable situations. The conditions set out in this paragraph serve as additional safeguards required for reuse, and not as authorisation for it. The provisions of this paragraph are without prejudice to the enhanced safeguards and preventive measures required under the Standard in respect of the personal data of individuals or groups in vulnerable situations.

RED IBEROAMERICANA DE PROTECCION DE DATOS

Red Iberoamericana
Rede Ibero-Americana

Financiado por la Unión Europea
NextGenerationEU

Documento financiado por la Unión Europea, en colaboración con la Fundación para la Internacionalización de las Administraciones Públicas (FIAP) en el marco de la Alianza Digital UE-ALC. Las opiniones y los argumentos expresados en este documento no reflejan necesariamente los puntos de vista oficiales de la Unión Europea, ni de sus Estados miembros.