Specific Guidelines for Compliance with the Principles and Rights that Govern the Protection of Personal Data in Artificial Intelligence Projects

RED IBEROAMERICANA DE PROTECCION DE DATOS

Text approved by the Entities of the Ibero-American Data Protection Network (RIPD, in spanish) in the session held on June 21, 2019, in the city of Naucalpan de Juarez, State of Mexico, Mexico.

This document was submitted for public consultation by the RIPD and the comments received were considered in the drafting of the final version.

RED IBEROAMERICANA DE PROTECCION DE DATOS

RED IBEROAMERICANA DE PROTECCION DE DATOS

Table of contents

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 01. Introduction

/ 01. Introduction

The advancement of new technologies in the current technological environment involves innovative and varied personal data treatment models, which are subject to monitoring and control by the personal data protection authorities in the world, in order to preserved that Development is accompanied by respect for people's freedoms.

Thus, among the topics of the international agenda in personal data protection we find, cloud computing; digital mining; massive data treatment known as big data; the connectivity of devices and appification in an internet of everything; the reliable and secure record of operations and transactions through cryptography, blockchain and smartcontract applications; process automation and the use of algorithms in industry and robotics; these are only examples of technological, computing and connectivity capabilities that are continually redefined.

Among the main trends in our digital environment is artificial intelligence, which has caused special interest in the industry and governments given the large number of applications in which it can be implemented and the results in the derived processes. As a consequence, the International Conference of Data Protection and Privacy Commissioners (ICDPPC) in its 38th edition, held in Marrakech, Morocco in 2016, began with the analysis and discussion around the protection of personal data and privacy in artificial intelligence and robotics.

Subsequently, in the framework of the 40th ICDPPC, which took place in 2018, in Brussels, Belgium, the “Declaration on ethics and data protection in Artificial Intelligence” was approved, establishing six guiding principles as fundamental values to preserve human rights in the development of artificial intelligence.

Later, during the XVII Ibero-American Data Protection Network meeting (EIPD, in Spanish), held on 21st of June 2019, in Naucalpan de Juárez, Mexico, the document entitled: *“Recommendations for treatment of personal data in artificial intelligence”* was approved by the members of the RIPD.

This document contains complementary and more detailed guidelines than those contained in the RIPD document: "*General recommendations for treatment of personal data in Artificial Intelligence*". Both these documents are framed within the normative instrument that constitutes the common reference for the entities that are members of the RIPD, which is the Standards for Personal Data Protection for Ibero-American States, approved in Santiago, Chile, in 2017.

RED IBEROAMERICANA DE PROTECCION DE DATOS

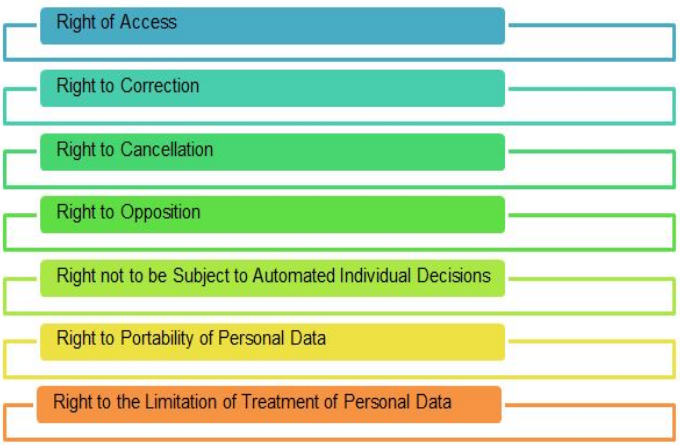
/ 02. Principles and Rights that Rule the Protection of Personal Data

/ 02. Principles and Rights that Rule the Protection of Personal Data

With the adoption of the Standards, a series of guiding principles and rights for the protection of personal data were recognized, that can be adopted and developed by the Ibero-American States in their national legislation in order to guarantee a proper treatment of personal data, and to have homogeneous rules in the region.

In accordance with the Standards, the guiding **principles** of personal data protection are:

Furthermore, the controller must guarantee and facilitate the data subjects the exercise of the following **rights**:



Summarising:

Taking into account the above, the following section carries out an analysis of the aspects that must be considered to comply with each of these principles and rights in treatment of personal data in the development of artificial intelligence.

RED IBEROAMERICANA DE PROTECCION DE DATOS

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 03. Specific Guidelines for Compliance with the Guiding Principles of the Protection of Personal Data

/ 03. Specific Guidelines for Compliance with the Guiding Principles of the Protection of Personal Data

The appropriate or due treatment of personal data must be carried out in compliance with various principles through which, person responsible and person in charge, will be able to prove its safe use, which includes the processing within the framework of AI applications, either as part of the processing or in its interaction with customers, administrators and other user profiles, as well as with other systems or applications.

Legitimation Principle (Article 11 of the Standards)

What is the Legitimation Principle?

In accordance with this principle, the person responsible may only treat personal data in the following assumptions:

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

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

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

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

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

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

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

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

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

/ 03. Specific Guidelines for Compliance with the Guiding Principles of the Protection of Personal Data

Specific guidelines for the legitimation principle in the treatment of personal data in the development of AI

- Consider, from the development of AI that carries out personal data processing, the implementation of simple, agile, effective and free mechanisms that allow to obtain the consent of holders, and if possible, to implement them prior to the use of AI.

- To comply with this commitment acquired through the Standards and for treatment to be lawful, the data must be treated with the consent of holder or, based on some other legitimate basis, such as public interest, a contractual need, compliance of legal obligations, and the vital interest of the individual, or scientific research. When applying any of these legitimate bases in the treatment, the compliance with the guiding principles governing the protection of personal data must be observed.

- In case it is considered necessary to obtain the consent of holder, it is recommended that it be:
    - Free: That there is no error, bad faith, violence or intent that may affect the manifestation of holder's will.
    - Informed: That holder has knowledge of treatment to which its personal data will be submitted and that knows the consequences of granting its consent.

- To obtain consent, the following options can be considered, as long as it does not contradict the provisions of the national legislation of the country in question:

    - Tacit consent: Tacit consent is obtained if holder do not refuse to have their personal data processed, after having known the privacy notice. That is, it is not necessary to be registered that holders authorized treatment of their personal information, but it is sufficient that they do not refuse treatment.

/ 03. Specific Guidelines for Compliance with the Guiding Principles of the Protection of Personal Data

- Explicit consent: Holder must expressly indicate that its consent to treatment of their personal data. Holder's will be expressed by an oral or written statement, including by electronic means, an oral statement, by optical, unambiguous signs or any other technology.
- Explicit-written consent: it must be granted in writing, by signature, fingerprint, electronic signature of the holder or any other authorized mechanism that allows data subject to be fully identified.

- When it is considered necessary to obtain consent, the request must always be limited to the specific purposes or compatible purposes of treatment that are being informed to holder, which means consent must be given to process personal data for specific purposes, not in general.

- Consent should be given before the collection of personal data or at the time indicated by the applicable regulations.

- Provide holder with simple and free means so that it can give or withdraw consent for treatment.

- When it is intended to further process personal data for purposes which are not compatible or analogous to those initially established, consent must be given by holder.

- If the automated decisions involve special categories of data, such as sensitive data, personal data should only be processed if holder has given its consent or if the applicable law contemplates exceptions to consent that allow treatment in a legitimate manner.

- When applicable, keep record of the consent given by holder for treatment.

- Be able to identify holders who did not give their consent for treatment for specific purposes, as long as these are not the ones that originate and sustain the legal relationship between the data subject and the person responsible.

/ 03. Specific Guidelines for Compliance with the Guiding Principles of the Protection of Personal Data

- In the cases of personal data of boys, girls and adolescents, the person responsible must verify whether the national legislation allows the minor to directly give consent for the treatment of their data or, obtain it from the holder of parental rights or guardianship according to the criteria established in the applicable national law.

Lawfulness Principle (Article 14 of the Standards)

What is the Lawfulness Principle?

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

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

Specific guidelines for the lawfulness principle in the treatment of personal data in the development of AI

- Know the regulations that specifically apply to the activity in which personal data is being processed and perform treatment in full compliance with it. Additionally, it is recommended to review the jurisprudence and soft law instruments in the field of human rights that may be applicable to the specific case.

- If the person responsible belongs to the public sector, the personal data must be treated according to the powers or functions that the regulations grant them.

- Check whether there is regulation that directly or indirectly applies to the protection or processing of personal data, such as health, financial and / or banking provisions.

- Include provisions on the obligation to comply with this principle in clauses, contracts or other legal instruments signed with third parties.

/ 03. Specific Guidelines for Compliance with the Guiding Principles of the Protection of Personal Data

Loyalty Principle (Article 15 of the Standards)

What is the loyalty principle?

This principle implies that the person responsible shall treat the personal data in its possession privileging the protection of holder's best interests and refraining from treating the data through deceptive or fraudulent means.

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

Specific guidelines for the loyalty principle in the treatment of personal data in the development of AI

- Avoid using deceiving or fraudulent means to process personal data and always do it in strict accordance with the ethical principles of AI of harm prevention and loyalty.
- Perform treatment of personal data respecting the interests of holder.
- Take into account the reasonable expectations of privacy of individuals in relation to the use of personal data and consider the impact of AI on society in general. Systems must be developed in a way that facilitates human development and does not obstruct or endanger it.
- When automated decisions are applied, it is recommended to implement measures to protect the rights, freedoms and legitimate interests of holder.
- The AI model should not emphasize information related to racial or ethnic origin, political opinion, religion or belief, union affiliation, genetic status, health status, sexual orientation, economic status, gender or the existence of any disability if this leads to arbitrary and discriminatory treatment.
- Establish a constant monitoring system of the AI model in order to identify the existence of biases and, when possible, implement a risk management system. As a final product, the monitoring system should generate reports and statistics that allow the person responsible to analyse the results.
- Bear in mind that the interconnection of different types of personal data may reveal confidential information about individuals.

/ 03. Specific Guidelines for Compliance with the Guiding Principles of the Protection of Personal Data

- Reduce and / or mitigate prejudices or discriminations that may result from the use of data in AI, prioritizing respect for international human rights law and non-discrimination instruments.

- Ensure that AI systems are designed in a way that facilitates human development, through an approach aimed at avoiding and mitigating the potential risks of personal data treatment.

- Prevent decision making through an AI technology from increasing the structural inequalities found in society and / or generating damage or suffering to data subjects individually or collectively.

- When the person responsible uses artificial intelligence for treatment of personal data, it should not "deceive" holder on whether it is an individual or just artificial intelligence doing treatment.

Transparency Principle (Article 16 of the Standards)

What is the transparency principle?

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

Therefore, the person responsible shall provide holder with at least the following information:

- Its identity and contact information

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

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

/ 03. Specific Guidelines for Compliance with the Guiding Principles of the Protection of Personal Data

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

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

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

Finally, every person responsible shall have transparent policies for the treatment of the personal data that it performs.

Specific guidelines for transparency principle in the treatment of personal data in the development of AI

- Communicate to the holder the main characteristics of treatment to which their personal information will be submitted.

- Expressly inform holders that automation processes will be used in treatment of their personal data.

- Include in the selected mean by the person responsible for complying with the principle of transparency, all the purposes for which the data of holders will be processed.

- In addition to the essential information that has to be informed to holder, in the event that personal data is subjected to automated processing, it is suggested as a good practice to continuously inform holders so that they can know the way in which automated decisions can affect them, and when necessary request human intervention, so they can make an informed decision as to whether or not to consent the treatment.

- The information provided regarding the logic of the AI model must include at least basic aspects of its operation, as well as the weighting and correlation of the data, written in a clear, simple and easily understood language, it will not be necessary to provide a complete explanation of the algorithms used or even to include them. The above always looking not to affect the user experience.

/ 03. Specific Guidelines for Compliance with the Guiding Principles of the Protection of Personal Data

- Promote transparency in AI through the development of innovative ways to inform holders of the main characteristics of treatment, and the level of risk related to the increase of privacy expectation.

- Safeguard the right to informational self-determination, by ensuring that holders are always informed in an adequate and timely manner that they will be interacting directly with an AI system or when their information will be treated by it.

- Provide significant information on the purpose and effects of AI systems to verify continuous alignment with the privacy expectation of holders, allowing them to exercise control over treatment of their personal data at all times.

- The use of AI challenges the person responsible to be as innovative in this area as they are when using analysis, and to find new ways to convey information concisely. There are several innovative approaches to providing privacy notices, including the use of videos, cartoons and standardized icons. The use of a combination of approaches can help make complex AI information easier for data subjects to understand.

- Identify and define commonly used terms and create a database so that they can be reused in different contexts, with standard icons[1] to make information known to the data subjects.

- Person responsible should be transparent about treatment of personal data by using a combination of innovative approaches in order to provide significant privacy notices at the appropriate stages throughout the AI project.

- Inform the origin of the personal data when they are obtained through a data transfer, and in case they are intended to be used for AI, validate that this purpose has been informed by the first person responsible who obtained them in order to make use of the data for that purpose.

Purpose Principle (Article 17 of the Standards)

What is the purpose principle?

In accordance with this principle, every treatment of personal data shall be limited to compliance with defined, explicit and legitimate purposes.

1. In this regard, the GDPR in paragraph 60 indicates that the information provided in compliance with the principle of transparency may be transmitted in combination with standardized icons that provide in an easily visible, intelligible and clearly legible way, an adequate overview of the intended processing.

/ 03. Specific Guidelines for Compliance with the Guiding Principles of the Protection of Personal Data

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

Finally, further treatment of personal data with filing, scientific or historical research or statistical purposes, all of them in favour of public interest, shall not be considered incompatible with the initial purposes.

Specific guidelines for the purpose principle in the treatment of personal data in the development of AI

- To explicitly consider the use of AI among the purposes for the processing of personal data.

- Recognise the purposes of treatment at the earliest possible stage of AI development and communicate it to holders in a colloquial language, so that it is understandable to the target population how their data is used.

- Ensure that the use of AI systems is consistent with the original purposes that motivated treatment so that personal data is not used for purposes incompatible with those that gave rise to its collection.

- When the person responsible identifies compatible and proportional purposes to those that gave rise to treatment, holders must be informed so that they are able to make informed decisions in this regard.

- Consider whether in the particular case in which it is intended to use AI it is a treatment for scientific research purposes[2] in favour of the public interest, since in that situation it will not be considered incompatible with the initial purposes.

- When a dynamic or online model is used in AI[3], given the nature of these, special care must be taken when making the data subjects aware of the purpose for which personal data will be disclosed.

2. With regard to the term scientific research, there are difficulties regarding the conception of what is meant by it, so that the provisions of the national legislation of the Ibero-American States applicable in the matter must be followed. In this regard, it is suggested to consult what the GDPR in paragraph 159 indicates for scientific research, as well as the rules provided in its article 89.

3. As a reference on dynamic or online models, it is suggested to consult the Report on “Artificial Intelligence and Privacy” for 2018, prepared by the Norwegian Data Protection Authority.

/ 03. Specific Guidelines for Compliance with the Guiding Principles of the Protection of Personal Data

Proportionality Principle (Article 18 of the Standards)

What is the proportionality principle?

In accordance with this principle, the person responsible shall only treat personal data that is appropriate, pertinent and limited to the minimum necessary regarding the purposes that justify their treatment

Specific guidelines for proportionality principle in the processing of personal data in the development of AI

- Collect and process the minimum quantity of personal data for AI, remember that it is better to have quality data than quantity.
- Evaluate if the data collected are necessary for the purposes that were informed to holders.
- If possible, it is suggested to implement AI that does not require the processing of personal data for its operation.
- Limit the period of processing personal data to the indispensable minimum, especially if it is sensitive.
- Make use of pseudonymisation or encryption techniques to protect the identity of the holder, in such a way that the degree of intervention or impairment of their right to privacy and data protection is limited.
- For AI developers, it is suggested to examine the area of application envisaged for the model in order to facilitate the selection of data that is adequate, pertinent and relevant for the intended purpose.
- AI developers should critically assess the quality, nature, origin and amount of personal data used, reducing unnecessary, redundant or marginal data during the development and training phases, and then monitor the accuracy of the model to as it feeds with new data[4].
- The use of synthetic data[5] can be considered as a possible solution to minimize the amount of personal data processed by AI applications.

4. Guidelines on Artificial Intelligence and Data Protection of the Consultative Committee of the Convention for the protection of individuals Regard to the Automated Processing of Personal Data.
5. For a definition of synthetic data go to: http://ec.europa.eu/eurostat/ramon/coded_files/OECD_glossary_stat_terms.pdf.

/ 03. Specific Guidelines for Compliance with the Guiding Principles of the Protection of Personal Data

- When AI is being developed consider the possibility of achieving the objectives in a less invasive way for holders. .

- In the event that it is intended to implement AI, it is suggested to perform impact assessments on the protection of personal data and document them, so that, at a specific time, they can be submitted to the Data Protection Authority in the case of an inspection or if a controversy arises in this regard in accordance with the provisions of section 41.1 of the Standards.

- Although it is difficult to establish the exact information that will be necessary and relevant for the development of an algorithm in AI, and this could be modified, it is important to continuously undergo evaluations to identify if that particular information is still necessary, in order to comply the minimization criteria.

- Performing periodic analyses regarding the appropriateness or relevance of personal data not only protects the reasonable expectation of privacy of holder, but also minimizes the risk in AI that irrelevant personal information leads the algorithm to find correlations that, instead of being significant, are coincidental and do not provide added value.

- Finally, the principle of proportionality plays an important role in the development of AI, to the extent that its effective application will protect the right to data protection of holders, impacting positively on building confidence in its use.

Quality Principle (Article 19 of the Standards)

What is the quality principle?

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

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

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

/ 03. Specific Guidelines for Compliance with the Guiding Principles of the Protection of Personal Data

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

Specific guidelines for the accuracy principle in the in the development of AI

- Periodically review algorithms that use AI so that the data that is processed for decision making is kept accurate, complete and up to date.
- Accurately classify information using data categories, so that the AI system makes correct predictions, recommendations or decisions based on data and models.
- Establish measures and mechanisms to avoid altering the veracity of the information, especially for AI processes that generate knowledge bases.
- Establish time limits for the preservation of personal information in AI systems and the storage media that contains it, considering that personal data must be deleted, destroyed, or deleted when there is no longer valid, legitimate or lawful reason for its conservation.
- Destruction of storage media containing personal data in AI systems should be done using secure erase methods and techniques, based on standards and best practices, to ensure that data cannot be recovered and used improperly.
- Establish periodic communication processes with officials or public authorities to improve data governance.

Responsibility Principle (Article 20 of the Standards)

What is the responsibility principle?

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

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

/ 03. Specific Guidelines for Compliance with the Guiding Principles of the Protection of Personal Data

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

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

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

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

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

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

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

g. Establish procedures to receive and answer questions and complaints from holders.

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

Specific guidelines for responsibility principle in the treatment of personal data in the development of AI

- In the development and use of AI technology, ensure compliance with the principles established in the Standards, and must adopt the necessary measures for its application, in addition to implementing mechanisms to prove compliance, this will apply even if in treatment of the data through this technology, a third party intervenes at the request of the person responsible.

- For compliance with the principles established in the Standards, the person responsible and the AI technology developers may use standards, international best practices, corporate policies, self-regulation schemes or any other mechanism that is determined appropriate for such purposes.

- Determine clear responsibilities and obligations of each of the actors involved in the process of design, development, implementation and use of technology.

/ 03. Specific Guidelines for Compliance with the Guiding Principles of the Protection of Personal Data

- Prevent decision making through an AI technology from increasing the structural inequalities found in society and / or generating damage or suffering to individuals or groups of people.
- Review AI systems to avoid producing biased social results, amplifying human bias or serving as a pretext for making biased decisions.
- The person responsible shall ensure that the services provided by any person in charge that processes personal data through AI technology, comply with the provisions of article 34 of the Standards.
- Keep the documentation that supports the selection of data, how the algorithm was developed and if it was properly tested before it was placed into use.
- Constantly supervise the activities carried out by external providers that offer AI services that involve treatment of personal data.
- Consider the creation of standards for the industry, code of ethics, as well as forums with experts in the fields of technology and personal data protection that provide advice on legal, ethical, social, technological challenges and opportunities related to use of AI.
- Adopt self-regulation schemes or good practices treatment of personal data through AI technologies.
- Perform regular evaluations of the AI systems to ensure that they comply with regulatory requirements.
- Remember that within ethical principles that must be observed in AI systems is the explainability principle, which is necessary to build and maintain the trust of users of AI systems, this seeks to make the processes transparent, that the capabilities and purposes of the AI systems are communicated openly and the decisions are explained, as far as possible, to those directly or indirectly affected in order to be accountable with the holder on treatment of their personal data.

Safety Principle (Article 21 of the Standards)

What is the safety principle?

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

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

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

b. The state of the technique.

/ 03. Specific Guidelines for Compliance with the Guiding Principles of the Protection of Personal Data

c. The costs of application.

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

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

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

g. The number of holders.

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

i. Prior violations to the treatment of personal data.

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

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

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

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

The notice referred to in the previous paragraphs shall contain, at least, the following information:

a. The nature of the incident.

b. The compromised personal data.

c. Corrective actions taken immediately.

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

/ 03. Specific Guidelines for Compliance with the Guiding Principles of the Protection of Personal Data

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

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

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

Specific guidelines for safety principle in the treatment of personal data in the development of AI

- Involve stakeholders throughout the life cycle of the AI system, in order to decide together, the solution regarding the differences between the principles of personal data protection and the requirements of the AI system.
- Adopt a data governance framework that promotes the design, structure and supervision of AI technologies by interacting during personal data treatment.
- Identify, evaluate, document and continuously communicate policies, concessions, and solutions, regarding the established data governance framework.
- Evaluate and document the risks identified at the beginning of an artificial intelligence development and throughout the data life cycle, in order to provide for security measures to avoid any unwanted adverse impacts.
- Develop robust AI systems with a risk prevention approach, so that they are reliable in order to minimize unintended, unexpected and unacceptable damage.
- Adopt resilience against security attacks for AI systems, in order to protect against vulnerabilities that can be exploited by attackers.
- Establish administrative, physical and technical security measures, proportional to the magnitude of the risk posed in the different treatment of personal data in AI and depending on the capabilities of the system.

/ 03. Specific Guidelines for Compliance with the Guiding Principles of the Protection of Personal Data

- Ensure that the development, deployment and use of AI systems meet requirements such as: human supervision, technical robustness and security, privacy and data governance, transparency and accountability.
- Facilitate data traceability and conduct audits of AI systems, especially in critical contexts or situations.
- Promote training and education so that all interested parties are informed and trained in reliable AI.

Principle of confidentiality (Article 23 of the Standards)

What is the principle of confidentiality?

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

Specific guidelines for confidentiality principle in the treatment of personal data in the development of AI

- Avoid the dissemination of personal data treated using AI technology, without the consent of the holder.

- Maintain the secrecy of information related to personal data treated using AI technology, except when its communication is permitted by a legal provision.

- Clearly define the authorized personnel of the organization to have access to the AI technology that processes personal data, or the third parties acting on behalf of and for the person responsible. In this regard, the use of contractual clauses that define the obligations of employees within the organization, as well as the person in charge is recommended.

- Implement security measures necessary to ensure the secrecy of personal data treated through AI technology.

- Consider the pseudonymisation or anonymization of personal data if AI technology allows it without impacting its operation.

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 04. Specific Guidelines for Compliance with Obligations by Person Responsible and in Charge (Articles 33 and 34 of the Standards)

/ 04. Specific Guidelines for Compliance with Obligations by Person Responsible and in Charge (Articles 33 y 34 of the Standards)

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

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

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

In any case, the agreement or legal instrument shall establish at least, the following general clauses related to the services provided by the person in charge:

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

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

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

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

e. Maintain the confidentiality regarding the treated personal data.

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

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

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

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

/ 04. Specific Guidelines for Compliance with Obligations by Data Processors (Articles 33 y 34 of the Standards)

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

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

Specific guidelines for the person responsible - person in charge relation in the treatment of personal data in the development of AI

- Constantly supervise the activities carried out by external providers that offer AI services that involve treatment of personal data.

- Include in the contracts or legal instruments specific instructions[6] regarding the way in which personal data can be used by the person in charge and the specific purposes for their processing, this is due to the complexity of clearly distinguishing between the person responsible and the person in charge in the development of AI.

6. It should be taken into account that if the organization entrusted with the analysis of data for the development of AI has sufficient freedom and experience to decide what data is obtained and how to apply its own analytical techniques, it becomes a person responsible.

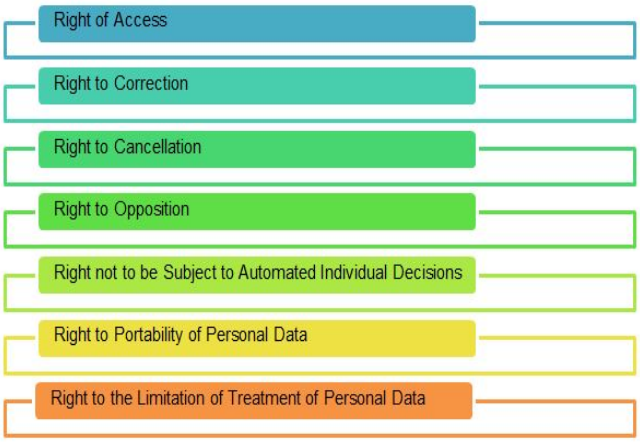
RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 05. Specific Guidelines for the Fulfillment of Rights (Articles 24 to 32 of the Standards)

/ 05. Specific Guidelines for the Fulfillment of Rights (Articles 24 to 32 of the Standards)

What are the rights of the holder?

The right to the protection of personal data allows individuals to have control over their personal information. The Standards recognize the rights of holders regarding treatment of their personal data, which are:



What is the right of access?

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

What is the right to correction?

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

What is the right of cancellation?

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

What is the right to opposition?

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

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

b) The purpose of the treatment of its personal data is direct marketing, including preparing profiles, to the extent that it related to such activity. When holder opposes treatment for direct marketing purposes, their personal data will no longer be processed for such purposes.

What is the right not to be subject to automated individual decisions?

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

/ 05. Specific Guidelines for the Fulfillment of Rights (Articles 24 to 32 of the Standards)

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

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

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

What is the right to portability of personal data?

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

For the exercise of this right, it should be taken into account that:

- Holder may request that its personal data are transferred directly from person responsible to person responsible when technically possible;
- The right to data portability will not adversely affect the rights and freedoms of others.
- Without prejudice to holder's rights, the right to portability of personal data shall not be admissible in the case of inferred, derived, created, generated information or information obtained from the analysis or treatment performed by the person responsible, based on the personal data provided by holder, such as personal data that had been subject to a personalization, recommendation, categorization or profile creation process.

What is the right to limitation of treatment of personal data?

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

/ 05. Specific Guidelines for the Fulfillment of Rights (Articles 24 to 32 of the Standards)

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

Specific guidelines for the attention of requests for the exercise of rights in treatment of personal data in the development of AI

- Inform holder when they interact with an AI application.
- Ensure that AI systems allow the exercise of rights, establishing simple, expeditious, accessible and free means and procedures in compliance with the provisions of the Standards.
- Ensure that the development of AI is programmed in such a way that when a data subject exercises any of these rights, the person responsible can comply with what is requested in an orderly manner.
- In the exercise of the right of access: allow holders to know the logic of the algorithms used in AI, for example, explaining, if possible, the variables used and their weighting; report on the type of expected input and output data; consider the implementation of mechanisms for holders to verify their profile, including details of the information and sources used to develop it.
- Consider including tools for the administration of preferences, such as a privacy panel, so that, through it, holders can manage what happens with their information in the various services, they can also modify the configuration, update their personal data, and review or edit their profile to correct any inaccuracies.
- Inform holders about the underlying reasoning in the AI data treatment operations that apply to them. When possible, the consequences of such reasoning should also be informed.
- Recognize the right of data subjects not to be the subject of a decision based solely on automated treatment if it affects them significantly and guarantee the right of individuals to challenge such decision if that is the case.
- When using automated treatment, recognize to the holder the right to obtain human intervention, so that he or she can receive an explanation of treatment and express its point of view, always respecting their reasonable expectation of privacy.
- Have tools that simply allow holders to carry their personal data in case it is viable through AI technology[7].

7. Guidelines on the right to data portability https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 06. Specific Guidelines for the Application of Proactive Measures in Treatment of Personal Data of AI Projects

/ 06. Specific Guidelines for the Application of Proactive Measures in the Processing of Personal Data AI Projects

The implementation of proactive measures in treatment of personal data in the national legislation of the Ibero-American States will seek to promote the best compliance with its legislation and help strengthen and increase the controls for the protection of personal data implemented by the person responsible.

Privacy by design and privacy by default (Article 38 of the Standards)

What is privacy by design and by default?

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

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

Specific guidelines for privacy by design and by default in the treatment of personal data in the development of AI

- From the design of AI in the program, system, platform or any other technology that involves treatment of personal data, the controller must apply measures that enable the effective compliance of the obligations derived from the applicable regulations regarding personal data.

- When AI is being developed, consider the possibility of achieving the objectives in a less invasive way for holders, in terms of ethics, compliance with principles and valuing the relationship between usability and privacy.

- Recognize the importance of embedding privacy as a requirement in the design and architecture of the program, service, system, platform or any other AI technology, with the objective of proposing technical measures for the identified privacy risks before they materialize.

/ 06. Specific Guidelines for the Application of Proactive Measures in the Processing of Personal Data AI Projects

- Consider that AI developers adapt the logic of the algorithms, so that the AI systems guarantee by default the security of personal data and thus comply with the obligations in the matter.

Impact assessment on the protection of personal data (Article 41 of the Standards).

What is the Impact Assessment on the protection of personal data?

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

That is to say, the person responsible will perform a documented analysis through which if it intends to put into operation or modify public policies, programs, systems or computer platforms, it will assess the real impacts with respect to certain treatment of personal data, in order to identify possible risks for the data, and know the measures implemented and to be implemented to protect them and mitigate the identified risks.

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

Specific guidelines for Impact Assessment on the protection of personal data when treat personal data in the development of AI

- Perform an Impact Assessment on the protection of personal data provided that any of the following takes place:

  - o Personal data is processed.
  - o The use some kind of artificial intelligence that could be perceived as particularly intrusive of privacy.
  - o The public policy, program, system or electronic platform in which it is intended to develop AI, yields results that could lead to the taking of actions or decisions with an impact or affectation to the holders.

/ 06. Specific Guidelines for the Application of Proactive Measures in the Processing of Personal Data AI Projects

38

- Elaborate the risk identification, which includes the following elements:

    - o Evaluate the need for treatment operations in the use of AI, as well as its proportionality in relation to the purposes of the public policy, program, system or electronic platform being developed.
    - o Identify, in the context of the use of AI, the potential risks for holders, including those derived from the analysis of sensitive personal data.
    - o Evaluate the potential risks to the rights and freedoms of holders protected by the applicable regulations of each country.

- Evaluate the measures implemented and to be implemented to mitigate the risks identified in the use of AI.

- Periodically evaluate treatment operations with AI, in order to determine if the measures implemented to mitigate the risks of its use are functioning as expected.

- Document the privacy impact assessments that are carried out, so that, at a specific time, they can be submitted to the competent Data Protection Authority, in the case of an inspection or if a dispute arises in this regard.

/ 07. Glosario

EIPD

Ibero-American Data Protection Meeting

Standards

Standards for the Protection of Personal Data for Ibero-American States

AI

Artificial Intelligence

RIPD

Ibero-American Data Protection Network


RED
IBEROAMERICANA DE
PROTECCION
DE DATOS