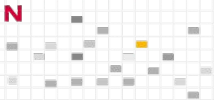
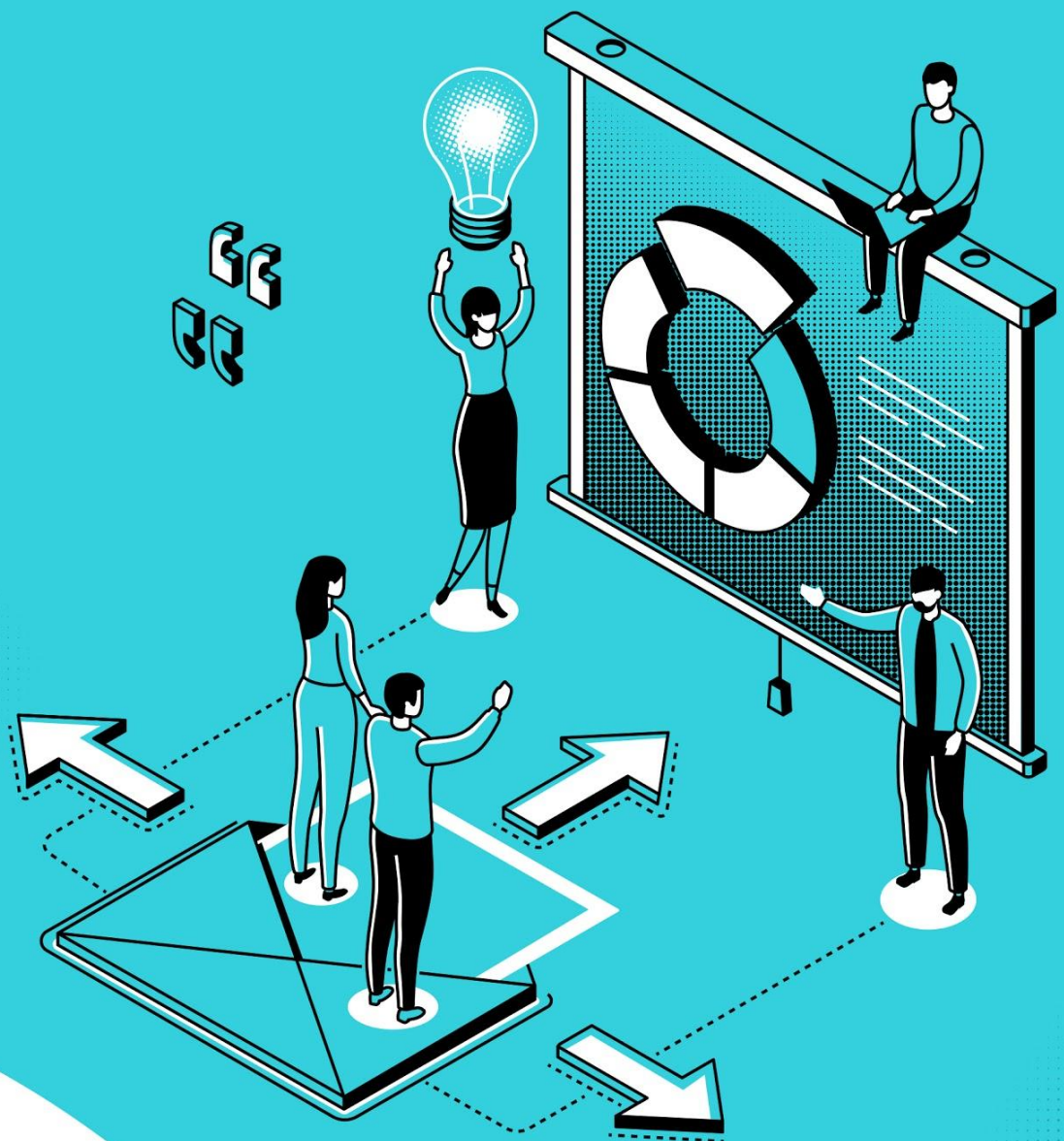


# General Recommendations for the Processing of Personal Data in Artificial Intelligence



Document approved by the Entities member of the Ibero-American Data Protection Network in the 21 June 2019 session in Naucalpan de Juárez, Mexico.

This document was subject to public consultation on behalf of the Ibero-American Data Protection Network and the observations received were considered in this final version.



# Table of contents

	Page
<b>01. Introduction</b>	<b>5</b>
<b>02. Objectives and Precisions</b>	<b>7</b>
<b>03. ¿Who are the Actors Involved in the Treatment of Personal Data Used in AI?</b>	<b>10</b>
<b>04. Impact of Data Protection Regulation in Artificial Intelligence</b>	<b>12</b>
<b>05. Recommendations</b>	<b>14</b>
I. Comply with Local Regulation on the Treatment of Personal Data	15
II. Conduct a Privacy Impact Assessment	15
III. Embed Privacy, Ethic, and Security by Design and by Default	16
IV. Materializing the Principle of Accountability	18
V. Design Appropriate Governance Structures in Organizations Developing AI Products	19
VI. Adopt Measures to Guarantee the Observance of Data Protection Principles	19
VII. Respect the Holder's Rights and Implement Effective Mechanisms for the Exercise of Said Rights	20
VIII. Ensure Data Quality	22
IX. Use Anonymization Tools	22
X. Increase Holders' Trust and Transparency	22
<b>06. Acronyms</b>	<b>23</b>
<b>07. Documents Consulted</b>	<b>24</b>



## / 01. Introduction



Artificial Intelligence (“AI”) has generated various expectations with regards to its economical, scientific, and social impact. As such, it has been in the agenda of governments, industry, academia, civil society organizations, and Data Protection Authorities.

Although there is not one definition on AI, it can be affirmed that in its ample conception, it is an “umbrella” term that comprises a variety of computational techniques and processes that seek to enhance the capacity machines have to develop algorithms, to create machine learning systems, and to reach deep learning techniques. Particularly, AI is related to the use of algorithms, which are a group of rules or a sequence of logical operations in order for a machine to make a decision or act in a determined way.

Personal Data is essential to AI because it is a crucial input to the functioning of certain AI systems. In effect, AI involves the recollection, storage, analysis, processing, or interpretation of enormous quantities of information (big data), which is applied to generate results, actions, or behaviors in a machine.

There’s a growing concern related to the use of personal data in the development of AI; which is why respecting human rights and the applicable regulatory framework becomes more relevant every day. As such, when an AI software, product or machine requires in its development or functioning personal data, manufactures must respect special regulation on the subject; which is made up of local laws of the country in which they are operating, and principles and rights contained in documents published by international organizations.

When referring to personal data, it is important to take into account the interests of the Holder while at the same time recognizing data is necessary to develop activities which are licit, legitimate, and of general interest. Consequently, regulatory frameworks do not oppose the treatment of personal data, but requires it to be surrounded by adequate guarantees. To sum up, rules on the treatment of personal data seek to avoid the abuse of information that might generate a threat or violation of the rights of the holder.

---

1. Cfr. Royal Society ( “Machine Learning: The Power and Promise of Computers That Learn by Example,” Royal Society,



## / 02. Objectives and Precisions

---



## / 02. Objectives and Precisions



The objective of this document is to give recommendations to developers and manufacturers of AI, with the purpose of guiding them so that from the start of the design of the product, the minimum regulatory requirements on the treatment of personal data are met. As a result, these recommendations<sup>2</sup> only apply to personal data and not to other types of information.

The Standards for Personal Data Protection for Ibero-American States (“Standards”), published by the Ibero-American Data Protection Network (“RIPD” by its acronym in Spanish or “Network”), were used as a reference to establish principles, terms, and definitions, for the present document. Nevertheless, it is not a transcription of all the aspects of the document containing the Standards, since we only make an allusion to some of it. As such, this document must be read jointly, comprehensively and harmoniously with the aforementioned standards.

Furthermore, these recommendations have a preventive approach, since they are based on the assumption that the best way to protect human rights through the treatment of personal data is by avoiding its violation.

In order to know the details of the implementation of some of these recommendations, the RIPD has elaborated complementary and more specific guidelines contained in the document “Specific guidelines for compliance with the principles and rights that govern the protection of personal data in artificial intelligence projects”.

---

2. This Document is not an academic article or a legal concept nor does it constitute a legal consultancy. Additionally, it does not seek to give an exhaustive list of specific recommendations on all the topics involved in AI, which is why adopting the recommendations written in this Guidelines, entails tailoring the measures to meet the specific AI project of the implementing organization that intends to use them.





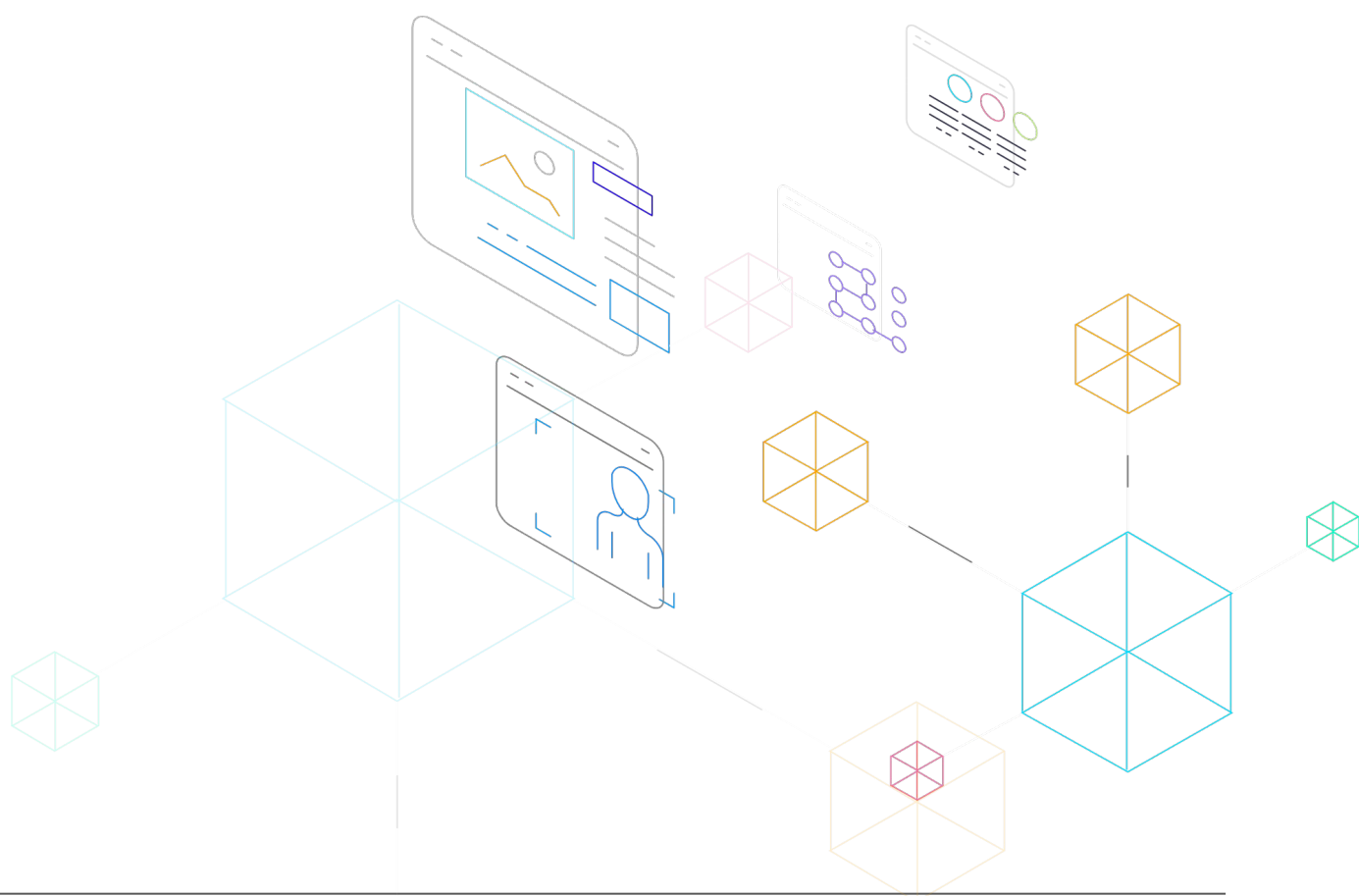
## / 03. ¿Who are the Actors Involved in the Treatment of Personal Data Used in AI?

---

## /03. ¿Who are the Actors Involved in the Treatment of Personal Data Used in AI?

According to the Network's Standards, the treatment of personal data refers to "any operation or set of operations performed through physical or automated procedures on personal data, related to, but not limited to, the collection, access, registration, organization, structuring, adaptation, indexation, modification, extraction, consultation, storage, preservation, development, transfer, dissemination, possession, exploitation, and in general, any use or disposal of personal data".

Given the aforementioned, there are various subjects involved in the treatment of the personal data and the protection of the rights of the Holder, such as: The person in charge; the person responsible; the exporter; the developers and manufactures of the technology, the software, or the algorithms; the holder; the providers of AI systems; and the Data Protection Authorities (DPA).



2. This Document is not an academic article or a legal concept nor does it constitute a legal consultancy. Additionally, it does not seek to give an exhaustive list of specific recommendations on all the topics involved in AI, which is why adopting the recommendations written in this Guidelines, entails tailoring the measures to meet the specific AI project of the implementing organization that intends to use them.

## / 04. Impact of Data Protection Regulation in Artificial Intelligence

---

## / 04. Impact of Data Protection Regulation in Artificial Intelligence

On the “Declaration on Ethics and Data Protection in Artificial Intelligence”<sup>3</sup> the link between collection, use, and disclosure of personal information and the advancement of artificial intelligence is recognized. Henceforth, it is necessary to make the following precisions: i) personal data is a legal category of information with special rules that must be observed in the development of artificial intelligence projects; ii) not every AI development implies the treatment<sup>4</sup> of personal data; and iii) personal data is not the only information collected, stored, analyzed or used in AI developments.

In this sense, when AI products use personal data, manufacturers must observe special regulation on the matter, which is made up of local norms of the specific country, and the group of principles and rights created by documents published by international organizations.

It is important to bear in mind that personal data regulation not only takes into account the interests of the holders, but it also recognizes the usefulness and necessity of data in the realization of diverse legal and legitimate activities. Consequently, regulation does not oppose the treatment of data, but it demands the treatment to be surrounded by adequate guarantess. To sum up, rules on the treatment of personal data seek to avoid any abuse that might generate a threat or violation to human rights



3. Cfr. “Declaration on ethics and data protection in artificial intelligence” 40th International Conference of Data Protection and Privacy Commissioners Tuesday 23rd October 2018, Brussels, Web:

[https://icdppc.org/wp-content/uploads/2018/10/20180922\\_ICDPPC-40th\\_AI-Declaration\\_ADOPTED.pdf](https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf)

4. Throughout this document, the words “treat” or “treatment” will be understood as any operation or set of operations performed through physical or automated procedures on personal data, related to, but not limited to, the collection, access, registration, organization, structuring, adaptation, indexation, modification, extraction, consultation, storage, preservation, development, transfer, dissemination, possession, exploitation, and in general, any use or disposal of personal data.



## / 05. Recommendations

12

The United Nations has emphasized on the importance to “make full use of scientific and technological developments for the welfare of man and to neutralize the present and possible future harmful consequences of certain scientific and technological achievements” . Moreover, it has recognized that “scientific and technological achievements<sup>5</sup> can entail dangers for the civil and political rights of the individual or of the group and for human dignity”.

As such, it is necessary to reach a point of equilibrium between innovation, development, AI, and human rights. There is no magical formula in order to fulfill this. However, there are certain recommendations that, when applied altogether, are useful in achieving said equilibrium. Above all, they are useful to reach a certain degree of social, economic, and technological development while respecting human rights.

With this purpose in mind, the RIPD gives the following recommendations to AI manufacturers or developers who must treat personal data:

### **1. Comply with Local Regulation on the Treatment of Personal Data.**

Although there is a globalized, hyperconnected world, national rules on data protection are not obsolete and have not disappeared; hence, complying with them is mandatory when working with AI. As a result, for an AI product not to be legally questioned, a legal risk study based on national regulations must be executed.

This will allow organizations to define a smart and efficient strategy to: (i) mitigate legal risks; (ii) Earn and maintain holders’ trust in AI technology; (iii) risk affecting the good reputation or good name of the organization; and (iv) avoid investigations and sanctions from the Data Protection Authority or any other state entity.

### **2. Conduct a Privacy Impact Assessment.**

Before designing and developing AI products, the organization shall conduct a Privacy Impact Assessment (PIA). The PIA will help organizations implement an effective risk management system while allowing them to adopt internal controls to guarantee that personal data is being processed in accordance with existing regulation. In this sense, the Standards state that “When the person responsible intends to perform a type of treatment of personal data that due to its nature, context or purposes probably entails

---

5. UN (1975), Op. cit



## / 05. Recommendations



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<sup>6</sup> .

The PIA should include, at least, the following:

- A detailed description of the operations that involve the processing of personal data in the development of AI;
- A risk assessment, specifically with regards to the rights and liberties of the data holder; and
- Measures implemented to mitigate risks, including guarantees, security measures, software design, technology and mechanisms. All these measures must be implemented taking into account the rights and interests of the data subjects as well as third parties that may be affected by this.

The results of the PIA, along with the measures taken to mitigate risks shall be implemented as part of the privacy by design and by default.

### 3. Embed Privacy, Ethic, and Security by Design and by Default.

Privacy by Design and by Default is considered a proactive measure in order to comply with the principle of accountability<sup>7</sup>.

As it can be observed in article 38 of the Standards, by embedding Privacy by Design (PbD), organizations seek to guarantee the privacy of the data used in AI processes, even before the materialization of the risks established in the PIA<sup>8</sup>. The best way to guarantee the due processing of personal data is by taking privacy as an essential component in the design and architecture of the software or the algorithm.

Privacy by Design “advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization’s default mode of operation<sup>9</sup>” . Consequently, even before collecting information and during its whole lifecycle, preventive measures of diverse nature (technological, organizational, human, and procedural) shall be adopted. Through this, organizations can avoid violating the right to privacy and confidentiality of the information of the data subjects.

Ethics by design and by default, must irradiate the whole scheme, development, and use of products or AI processes; thus, being part of the DNA of any AI project.

The aforementioned must also be said about security by design and by default when treating data in AI. Without safeguards there is no privacy in the rightful processing of personal data. It is of special importance to

---

6.Ibero-American Data Protection Network (2017), Article 41.1

7.Cavoukian (2011).

8.Gulbenkoglul (2018)

9.Cfr. Cavoukian (2011)

## / 05. Recommendations



adopt technological, human, administrative, physical and contractual measures in order to fulfill the following objectives:

- Avoid the wrongful or unauthorized access to data
- Avoid the manipulation of data
- Avoid the destruction of information
- Avoid the wrongful or unauthorized uses of data
- Avoid circulation of data to unauthorized people

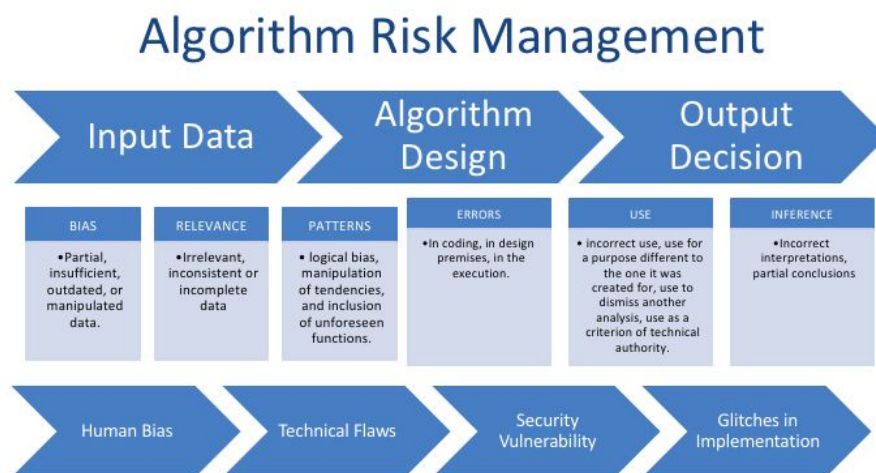
Safety measures must be appropriate and must take into consideration various factors, such as the following: (i) the levels of risk in the processing; (ii) the nature of the data; (iii) the magnitude of the harm that can be caused to the data subjects and the controller if the data is wrongly processed; (v) the size of the organization; (vi) the available resources; (vii) the monitoring of

the reliability of algorithms ; (viii) the state of the art; (ix) the context and finality of the treatment of data; (x) the cross border circulation of data; and (xi) the uncertainty and complexity of each AI initiative.

Said measures must be object of revision, evaluation, and permanent improvement.

Risks associated with AI systems must be subject to planification and mitigation efforts, proportional to the eventual gravity of the damages generated<sup>10</sup>. Amongst contingencies, organizations must consider the inherent risks of operating with algorithms (human bias, technical flaws, security vulnerabilities, and failures in their implementation) and their faulty design.

Regarding this, certain aspects affect the management and performance of the algorithm, as shown in the following graphic<sup>11</sup>:



## Inherent Risk Factors

10- Future of Life Institution (2017)

11. The image is an adaptation taken from the graphic published in: USECHE, Alejandro y CANO, Jeimy (2019). Robo-Advisors: Asesoría automatizada en el mercado de valores. Universidad del Rosario y Autorregulador del Mercado de Valores de Colombia

## / 05. Recommendations



According to doctrine, “the data input is affected mainly by two variables: bias (incorporation partial, insufficient, manipulated, or outdated data) and pertinence (relevance, inconsistency or completeness of the data). On the other hand, the development of the algorithm can be affected by patterns (programming logic bias, including not foreseen functions, and inherent failures of the functions used to codify) and errors (conditions of the operation that reflect a functioning different to the one planned). Lastly, risks in the output decisions are related to the pertinence and precision of the execution of the algorithm as a direct response to the analysis of the data input<sup>12</sup>.

### 4. Materializing the Principle of Accountability.

Designers and developers of AI products must adopt useful, appropriate and effective measures in compliance with legal obligations imposed by local regulation. However, it is not enough to comply, since organizations have to demonstrate the correct compliance of their duties. The measures taken by each organization should then be subject to permanent revision and evaluation in order to measure its efficacy with regards to compliance and the protection of personal data.

For the adequate implementation of said principle, the Standards recommend the following mechanisms:

- “a. Allocate resources for the implementation of programs and policies for the protection of personal data.
- b. Implement risk management systems related to the treatment of personal data.
- c. Prepare mandatory and enforceable personal data protection policies and programs, within the organization of the person responsible.
- d. Implement a training and updating program for personnel about obligations on personal data protection matters.
- e. Periodically review the personal data safety policies and programs, in order to determine the required modifications.
- f. Establish an internal and/or external supervision and surveillance system, including audits, in order to prove compliance with the policies for the protection of personal data<sup>14</sup>.
- g. Establish procedures for receiving and answering questions and complaints from holders.<sup>13</sup>”

---

13.Ibero-American Data Protection Network (2017), Article 20.3

## / 05. Recommendations

The challenges faced by organizations when complying with the principle of accountability is that this principle demands going beyond the issuance of documents or redaction of internal politics. Organizations must be able to demonstrate to the Data Authority the real and effective compliance when they perform their functions. Symbolic declarations of good intentions are not enough, concrete results with regards to the processing of personal data in AI projects must be documented.

In this sense, it is essential to periodically give specialized training to those who create the products within the organization, as to provide the expertise, guide, and tools required for the correct development of AI projects.

Identifying and classifying risks, while at the same time adopting measures to mitigate them, are key elements of the principle of accountability. In the aforementioned guide, it is of fundamental importance for organizations to develop and put in place a “system of administration of risks associated with the processing of personal data<sup>14</sup>” so that the organization can “identify, measure, control, and monitor all the situations exposed to risk in order to comply with data protection regulation”<sup>15</sup>.

### 5. Design Appropriate Governance Structures in Organizations Developing AI Products.

It is recommended for organizations to define a clear structure with functions and responsibilities that guarantee good corporate governance with respect to the treatment of personal data while complying with laws and the holders’ rights.

The main functions and responsibilities<sup>16</sup> that must be allocated are the following<sup>17</sup>:

1. Assess and manage the risks to personal data when deploying AI
2. Decide on appropriate AI decision-making models
3. Conduct maintenance, monitoring and review activities
4. Revise channels of communication with users or consumers.

### 6. Adopt Measures to Guarantee the Observance of Data Protection Principles.

It is necessary for the Person Responsible or Person in charge to provide efficient strategies to guarantee compliance with the principles of the treatment of data protection found in Chapter II of the Standards for Personal Data protection for Ibero-American States published by the RIPD<sup>18</sup>.

14. Cfr. Republic of Colombia. Superintendence of Industry and Commerce (2015)

15. Ibid

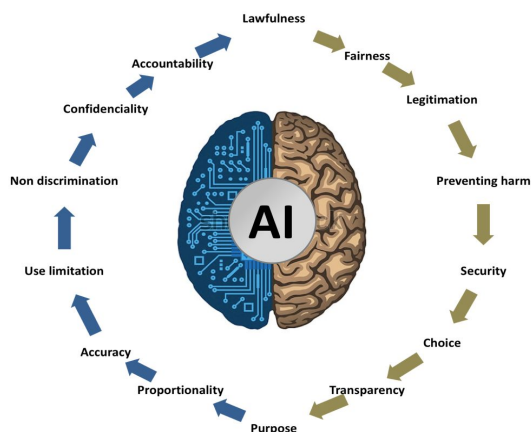
16. Singapore Personal Protection Data Commission (2019)

17. Singapore Personal Protection Data Commission (2019)

18. Ibero-American Data Protection Network (2017)

## / 05. Recommendations

30

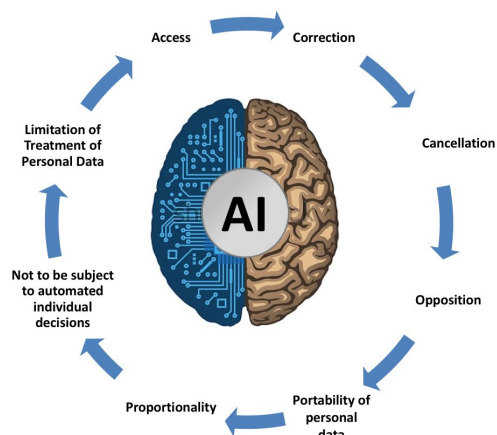


Graphic No. 1. Principles of the treatment of personal data relevant for the design and development of AI products

The scope of each principle is determined in the Standards published by the RIPD, which is why instead of transcribing it in this document, any additional information required can be found directly in the Ibero-American Data Protection Network Standards<sup>19</sup> for Data Protection document.

### 7. Respect the Holder's Rights and Implement Effective Mechanisms for the Exercise of Said Rights

The Fortieth (40th) International Conference of Data Protection and Privacy Commissioners, considered “that any creation, development and use of artificial intelligence systems shall fully respect human rights, particularly the rights to the protection of personal data and to privacy, as well as human dignity, non-discrimination and fundamental values, and shall provide solutions to allow individuals to maintain control and understanding of artificial intelligence systems<sup>20</sup>”.



Graphic No. 2. Rights of the Holders contained in Chapter III of the Ibero-American Standards for Data Protection published by the RIPD.

Given the aforementioned, organizations that create or use AI technology must guarantee the Holders, the following rights:

The scope of each right is determined in the Standards<sup>21</sup> published by the RIPD, which is why instead of transcribing it in this document, any additional information required can be found directly in the Ibero-American Data Protection Network Standards for Data Protection document.

Although all rights are equally important, we consider it pertinent to make the following reference to the right not to be subject to automated individual decisions:

According to Article 29 of the RIPD's Standards, the “Holder shall have the right not to be the subject of decisions that cause it legal effects, or that affect it in a significant way, based only on automated treatments intended to assess, without human intervention, some of his own personal

19. Ibero-American Data Protection Network (2017).

20. 40th International Conference of Data Protection and Privacy Commissioners–ICDPPC (2018).

21. Ibero-American Data Protection Network (2017).

## / 05. Recommendations

34

aspects, or to analyze and predict, specifically, its professional performance, economic situation, health status, sexual preferences, reliability or behavior". This general rule "shall not apply when the automated treatment of personal data is necessary for the execution of an agreement between holder and the person responsible; when it is authorized by the internal law of the Ibero-American States, or when it is based on provable consent from holder<sup>22</sup>".

The above-mentioned rule, only applies when there is no direct or indirect human intervention, since the purpose is to grant the Holder the possibility to controvert the automated decision before a human being; thus, not leaving the decision 100% in the hands of algorithms or automated processes. Consequently, when there is an automated decision, "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<sup>23</sup>".

Lastly, the Standards prohibit discriminatory automated decisions. In this sense, the rule states, "The person responsible may not perform automated treatments of personal data in its possession which purpose is holders' discrimination due to their racial or ethnic origin; beliefs or religious,

philosophical and moral convictions, union affiliation, political opinions; data related to health, life, sexual preference or orientation, as well as genetic or biometric data<sup>24</sup>".

It is necessary to highlight that the Standards oblige the person responsible to establish "simple, expeditious, accessible and free procedures that allow holder to exercise its rights to access, correction, cancellation, opposition and portability<sup>25</sup>". For this reason, AI developers must foresee a wide arrange of mechanisms for holders to exercise their rights.

Considering this, the ICDPPC's "Declaration on Ethics and Data Protection in Artificial Intelligence" emphasizes the need to promote the empowerment of each individual in the exercise of their individual rights and the creation of opportunities:

1. Respecting data protection and privacy rights, including where applicable the right to information, the right to access, the right to object to processing and the right to erasure, and promoting those rights through education and awareness campaigns,
2. Respecting related rights including freedom of expression and information, as well as non-discrimination,

22. Ibero-American Data Protection Network (2017), Article 29.2

23. Ibero-American Data Protection Network (2017), Article 29.3

24. Ibero-American Data Protection Network (2017), Article 29.4

25. Ibero-American Data Protection Network (2017), Article 32



## / 05. Recommendations

33

1. Recognizing that the right to object or appeal applies to technologies that influence personal development or opinions and guaranteeing, where applicable, individuals' right not to be subject to a decision based solely on automated processing if it significantly affects them and, where not applicable, guaranteeing individuals' right to challenge such decision,
2. Using the capabilities of artificial intelligence systems to foster an equal empowerment and enhance public engagement, for example through adaptable interfaces and accessible tools.<sup>26</sup>

### 8. Ensure Data Quality.

One of the biggest risks when developing and using AI is the risk of bias, which can be caused by a preconfiguration of the algorithm and the quality of the data collected. To minimize this bias risk and avoid violating holders' rights, the data used must be veridic and precise.

To reduce the bias risk, the following is recommended to: (i) keep a data provenance record<sup>27</sup>; (ii) carry out audits on the datasets used in the creation of algorithms. This will uncover mistakes and inherent limitations of the algorithms used in the decision-making processes conducted with AI; (iii) grant veracity scores to the datasets used to train the machine when created; (iv) regularly update the data being used to feed the

machine; and (v) have separate datasets to train, test, and validate the decision-making process.

### 9. Use Anonymization Tools.

It is important to establish in an AI project if it is strictly necessary for the data used to be associated or related to a particular person. If it's not necessary, it is recommended to use anonymized information in which the holder is not identified.

In this sense, anonymization helps reduce the risks inherent to the massive treatment of personal data in AI projects and processes.

### 10. Increase Holders' Trust and Transparency.

For the last decades, trust has become a crucial factor for the growth and consolidation of any economic activity developed through the use of technologies<sup>28</sup>, which has been reiterated as follows, *"continuous activities directed at creating trust must be one of the most important strategic priorities for an organization"*<sup>29</sup>

Trust must be understood as the expectation that "one can count with the other person's word" and that positive and beneficial actions will take place between the parties in a reciprocal manner. When there is trust, the holder believes the organization is reliable, honest, and keeps its word<sup>30</sup>.

26. 40th International Conference of Data Protection and Privacy Commissioners–ICDPPC (2018).

27. Singapore Personal Protection Data Commission (2018)

28. Cfr. Reichel & Shefter. Harvard Business Review. July to August 2000

29. Cfr. Edelman Trust Barometer de 2019

30. Cfr. Barrera Duque, Ernesto (2018) Diseño organizacional centrado en el cliente. Teoría y práctica en empresas sociales. Universidad de la Sabana y Ecoe ediciones.



## /05. Recommendations

33

A transparent organization can generate more trust to its clients and the holders by adopting the following suggestions:

- (i) Establish open communication channels that promote trust with consumers<sup>31</sup>. In order to do so, it is important for organizations, when possible, to divulge the use or role of AI in their product or services. This undoubtedly augments transparency. Additionally, when communicating with their users, organizations shall use easy-to-understand language so that any user, without previously acquired knowledge on artificial intelligence, can understand
- (ii) Conduct pilot tests<sup>32</sup> to evaluate the decision-making model and correct any problem before launching it. This is also important to guarantee that the user finds a friendly and functional interface.
- (iii) Additionally, the organization shall consider providing the consumer with the option to opt out<sup>33</sup>. Through this, the consumer can request that his information be excluded from the datasets, in cases permitted by the Law.
- (iv) Establish decision review channels<sup>34</sup> where decisions made by machines can be revised by humans, considering that algorithms have a risk of bias and unknown exceptions<sup>35</sup>.



31. Singapore Personal Protection Data Commission (2019)

32. Singapore Personal Protection Data Commission (2019)

33. Singapore Personal Protection Data Commission (2019)

34. Singapore Personal Protection Data Commission (2019)

25. Singapore Personal Protection Data Commission (2019)



## / 06. Acronyms

32

### **Standards**

Standards for Personal Data Protection for  
Ibero-American States

---

### **AI**

Artificial Intelligence

---

### **GDPR or General Data Protection Regulation**

European Union Regulation (EU) 2016/679 of the  
European Parliament and of the Council of 27 April  
2016 on the protection of natural persons with  
regard to the processing of personal data and on  
the free movement of such data, and repealing  
Directive 95/46/EC

---

### **RIPD or Network**

Ibero-American Data Protection Network



## / 07. Documents Consulted



1. “Artificial intelligence and privacy”. Office of the Victorian Information Commissioner.

Disponible en: <https://ovic.vic.gov.au/resource/artificial-intelligence-and-privacy/>

---

2. “Artificial intelligence and privacy, Report, January 2018”, Norwegian Data Protection Authority

Disponible en: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>

---

3. “Artificial Intelligence, Robotics, Privacy and Data Protection. Documento de trabajo de la 38ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad.

Disponible en:

[https://edps.europa.eu/data-protection/our-work/publications/other-documents/artificial-intelligence-robotics-privacy-and\\_en](https://edps.europa.eu/data-protection/our-work/publications/other-documents/artificial-intelligence-robotics-privacy-and_en)

---

4. Barrera Duque, Ernesto (2018) Diseño organizacional centrado en el cliente. Teoría y práctica en empresas sociales. Universidad de la Sabana y Ecoe ediciones.
- 

5. “Big data, artificial intelligence, machine learning and data protection” Information Commissioner Office

Disponible en:

<https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>

---

6. Cavoukia, Ann. Privacidad por Diseño: Los 7 principios fundamentales.

Disponible en:

<http://mediascope.nl/wp-content/uploads/2015/08/privacidad-por-dise%C3%B1o.pdf>

## / 07. Documents Consulted

38

### 7. Consejo de Europa (2019) Unboxing Artificial Intelligence: Ten Steps to Protect Human Rights.

Disponible en:

<https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64>

### 8. “Declaration on ethics and data protection in artificial intelligence” 40th International Conference of Data Protection and Privacy Commissioners Tuesday 23rd October 2018, Brussels

Disponible en:

[https://icdppc.org/wp-content/uploads/2018/10/20180922\\_ICDPPC-40th\\_AI-Declaration\\_ADOPTED.pdf](https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf)

### 9. “Ethics guidelines for trustworthy AI” High-Level Expert Group on AI (AI HLEG)

Disponible en:

<https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>

### 9. European Group on Ethics in Science and New Technologies (2018). “Statements on Artificial Intelligence, Robotics and ‘Autonomous’ Systems”

Disponible en:

[http://lefis.unizar.es/wp-content/uploads/EGE\\_Artificial-Intelligence\\_Statement\\_2018.pdf](http://lefis.unizar.es/wp-content/uploads/EGE_Artificial-Intelligence_Statement_2018.pdf)

### 10. Government of Canada (2019) “Directive on Automated Decision-Making”

Disponible en: <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592>

## / 07. Documents Consulted

30

**11.** “Guía para Titulares de los Datos Personales Volumen 1. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Disponible en:

<https://www.cinvestav.mx/Transparencia-y-RC/Transparencia-Proactiva/Guia-para-titulares-de-datos-personales>

**12.** “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”. Adoptadas por el Article 29 Data Protection Working Party el 3 de octubre de 2017 y revisadas el 6 de febrero de 2018.

Disponible en: <https://www.pdpjournals.com/docs/887862.pdf>

**12.** “Guidelines on artificial intelligence and data protection” del Comité Consultivo de la Convención para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal

Disponible en:

<https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6>

**13.** OCDE (2019) “Recommendation of the Council on Artificial Intelligence”

Disponible en:

<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

**14.** “Privacy and Freedom of Expression In the Age of Artificial Intelligence”

Disponible en:

<https://privacyinternational.org/report/1752/privacy-and-freedom-expression-age-artificial-intelligence>



## / 07. Documents Consulted

30

**15.** Red Iberoamericana de Protección de Datos -RIPD- (2017).  
Estándares de protección de datos personales para los Estados  
Iberoamericanos.

Disponible en:

[http://www.redipd.es/documentacion/common/Estandares\\_Esp\\_Con\\_logo\\_RIPD.pdf](http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf)

---

**16.** Reglamento (UE) 2016/679 Del Parlamento Europeo y del  
Consejo de 27 de abril de 2016 relativo a la protección de las  
personas físicas en lo que respecta al tratamiento de datos  
personales y a la libre circulación de estos datos y por el que se  
deroga la Directiva 95/46/CE

Disponible en:

<https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679>

---

**17.** “Réformer le droit à la vie privée à l'ère de l'intelligence  
artificielle”

Disponible en:

<https://www.nationalmagazine.ca/fr-ca/articles/legal-market/legal-tech/reforming-privacy-in-the-age-of-ai>

---

**18.** Superintendencia de Industria y Comercio (2015) “Guía para  
implementación del principio de responsabilidad demostrada  
(accountability)”

Disponible en:

<http://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada>

---

## / 07. Documents Consulted

34

**19.** United Kingdom. “Understanding artificial intelligence, ethics, and safety”

Disponible en:

<https://www.gov.uk/guidance/understanding-artificial-intelligence-ethics-and-safety>

---

**20.** USECHE, Alejandro y CANO, Jeimy (2019). Robo-Advisors: Asesoría automatizada en el mercado de valores. Universidad del Rosario y Autorregulador del Mercado de Valores de Colombia . Págs. 9-10.

Disponible en:

<https://www.amvcolombia.org.co/wp-content/uploads/2019/02/Robo-Advisors-Final.pdf>

RED  
IBEROAMERICANA DE  
PROTECCION  
DE DATOS

