DRAFT LAW

On the processing of personal data to protect the personality and dignity of natural persons

I, THE PRESIDENT OF THE REPUBLIC, Declare that the National Congress has decreed and I hereby approve the following Law:

CHAPTER I

INTRODUCTORY PROVISIONS

Art. 1 This Law regulates the processing of personal data, in order to protect the fundamental rights of freedom and privacy of natural persons.

Art. 2 This Law applies to any processing operations performed through totally or partially automated means, by a natural person or by a legal person under public or private law, regardless of the country where they are located and the country where the database is located, provided that:

I - The processing operation is performed within the national territory; or

II - The personal data subject to processing have been collected within the national territory.

§ 1 Personal data are regarded as collected in the national territory if their data subject was located in the national territory at the time of collection.

§ 2 This Law does not apply to any data processing that is:

I - Performed by a natural person for exclusively personal purposes; or

II - Performed for exclusively journalistic purposes.

§ 3 Public bodies and public entities are forbidden to transfer the personal data in the databases managed by them or to which they have access in the exercise of their legal competences for private entities, except in cases of third-party execution or through a concession and permission for a public activity that requires it, and exclusively for determinate and specific purpose.

Art. 3 Government-owned companies and mixed-economy companies acting on a competitive basis, subject to the provisions in Art. 173 of the Constitution shall have the same treatment given to private legal persons, under the provisions of this Law.

Sole paragraph. Public companies and mixed-economy companies, when implementing public policies and not acting on a competitive basis, shall receive the same treatment as public bodies and entities, under the terms of this Law.

Art. 4 Processing of personal data solely for purposes of public safety, defence, State security, research activities, or the repression of criminal offences, shall be governed by specific legislation, according to the general principles of the protection of the data subject's rights established in this Law.

Sole paragraph. The processing of data described in the in the main clause by a private person is forbidden, except in procedures performed under the supervision of a public legal person, which shall be specifically reported to the competent body.

Art. 5 For purposes of this Law, the following definitions apply:

I - personal data: any data related to an identified or identifiable natural person, including identification numbers, location data, or electronic identifiers;

II - processing: the set of actions pertaining to the collection, production, reception, classification, use, access, reproduction, transfer, distribution, transport, processing, archiving, storage, deletion, assessment or control of information, modification, blocking, or supply to third parties of personal data, by means of communication, interconnection, transfer, disclosure, or extraction;

III - sensitive data: personal data that disclose the person's racial or ethnic origin, religious, philosophical, or moral beliefs, political views, affiliation to trade unions or religious, philosophical, or political organisations, data pertaining to the person's health or sexual life, as well as genetic data;

IV - anonymous data: data pertaining to a data subject that cannot be identified by the controller for the processing or by any other person, taking into account the means that can be reasonably used to identify said data subject;

V - database: a structured set of personal data, located in one or several locations, on an electronic or physical support;

VI - data subject: the natural person to whom the personal data processed refers;

VII - consent: free, express, specific, and informed statement by which the data subject agrees to the treatment of his/her personal data for a specific purpose;

VIII - controller: the natural or legal person, under public or private law, that can make decisions pertaining to the processing of personal data;

IX - processor: the natural or legal person, under public or private law, who performs the processing of personal data on behalf of the controller;

X - data communication: transfer of personal data to one or more specified subjects other than they subject, in any form;

XI - interconnection: transfer of personal data from one database to another, whether they have the same owner or not, for similar or different purposes;

XII - disclosure: transfer of personal data to one or more unspecified subjects, other than their subject, under any form;

XIII -international data transfer: transfer of personal data to a foreign country;

XIV - dissociation: the act of modifying personal data so that they cannot be directly or indirectly associated with an identified or identifiable individual;

XV - blocking: the keeping of personal data or a database under temporary suspension of any processing operation;

XVI - cancellation: the removal of data or a set of data stored in a database, by any means;

XVII - shared data use: the communication, disclosure, international transfer, or interconnection of personal data or shared processing of personal databases by public bodies or entities and private entities specifically authorised to perform one or more types of processing delegated by said public entities; and

XVIII - person in charge: the natural person, specified by the controller, who serves as liaison between the data subjects and the relevant body.

Art. 6 Personal data processing activities shall comply with the following general principles:

I - Principle of purpose, by which the processing must be performed for legitimate, specific, and explicit purposes that are known to the data subject;

II - Principle of suitability, by which the processing must be compatible with the purposes sought and with the data subject's legitimate expectations, according to the context of the processing;

III - Principle of necessity, by which the processing must be restricted to the minimum required for the performance of the purposes sought, including relevant, proportional, and non-excessive data;

IV - Principle of free access, by which facilitated queries by the data subjects on the types of processing and on the integrity of their personal data must be ensured, free of charge;

V - Principle of data quality, by which the accuracy, clarity, and up-to-date nature of the data must be ensured, with the frequency required for the fulfilment of the purpose of the processing of the data;

VI - Principle of transparency, by which the data subjects must be given clear and adequate information about the performance of the processing¿;

VII - Principle of security, by which constantly updated technical and administrative measures, proportional to the nature of the information processed and suitable to protect personal data from non-authorised access and from accidental or unlawful destruction, loss, change, communication, or disclosure, must be used;

VIII - Principle of prevention, by which measures must be taken to prevent damage from personal data processing; and

IX - Principle of non-discrimination, by which the processing cannot be performed for discriminatory purposes.

§ 1 The public bodies shall announce their data processing activities by means of clear, precise, and updated information in easy accessible vehicles, preferably on its electronic websites, in compliance with the principle of transparency established in section VI.

§ 2 Shared use of personal data must comply with the specific purpose of execution of public policies and must be legally assigned by public bodies and entities, in compliance with the principles of purpose, suitability, and necessity established in sections I, II, and III.

CHAPTER II

REQUIREMENTS FOR PERSONAL DATA PROCESSING

Section I

Consent

Art. 7 Personal data processing is only allowed when free, express, specific, and informed consent is given by their data subject, except in the case described in art. 11.

§1 Consent for personal data processing shall not be a condition for the supply of a product or service or for the exercise of legal rights, except in cases in which personal data are required for these purposes.

§2 The processing of personal data obtained by error, fraud, state of need or coercion is forbidden.

§3 Consent shall be given in writing or by any other means that certifies it.

§4 Consent shall be given separately from the other contractual clauses.

§5 Consent shall pertain to specific purposes. Generic consent for personal data processing shall be invalid.

§6 Consent may be revoked at any time, free of cost to the data subject.

§7 Any provisions that establish unfair or abusive obligations to the data subject or provisions that place the data subject at significant disadvantage, or which are incompatible with good faith and equity, are void.

§8 The controller holds the burden of proving that the data subject's consent was obtained in accordance with the provisions set forth in this Law.

Art. 8 data subjects of personal data ages between twelve to eighteen may consent to the data processing that respects their condition as developing persons, without prejudice to the possibility of revocation of such consent by their parents or legal tutors, to protect their best interests.

Art. 9 In the case of data subjects of personal data who are not yet twelve years old, consent shall be given by their parents or legal tutors. The processing shall respect their condition as developing persons.

Art. 10 When consent is given, the data subject shall be clearly, adequately, and ostensibly informed about the following points:

I - Specific purpose of the processing;

II - Form and duration of the processing;

III - Identification of the controller;

IV - Controller's contact data;

V - subjects or categories of subjects to whom the data can be communicated, as well as the scope of disclosure;

VI - Responsibilities of the agents that will perform the processing; and

VII - data subject's rights, specifically mentioning:

a) The possibility of not giving consent, explaining the consequences of this refusal, pursuant to section § 1 in art. 6;

b) The possibility of accessing and modifying the data, as well as withdrawing their consent, by means of an easy and free of charge procedure; and

c) The possibility of filing a claim with the competent body for breach of the provisions in this Law.

§ 1 Consent is void if the information given is misleading or is not clearly, adequately, and ostensibly presented.

§ 2 In the event of a change in the information described in sections I, II, III and V of the main clause, the controller shall obtain a new data subject's consent, after specifically describing the nature of the changes.

§ 3 In the event of a change in the information described in section IV of the main clause, the controller shall communicate the updated data to the data subject.

§ 4 In activities involving ongoing collection of personal data, the data subject shall be regularly informed of their continuity, according to the terms defined by the competent body.

Art. 11. Consent is exempt in the case of unrestricted public access data, or whenever processing is necessary to:

I - The fulfilment of a legal obligation by the controller;

II - The shared use of data pertaining to the exercise of rights or duties established by law or regulation by the public authorities;

III - The execution of pre-contractual procedures or obligations related to an contract to which the data subject is party, pursuant to section § 1 of art. 6;

IV - The performance of historical, scientific, or statistical research, ensuring, whenever possible, the dissociation of the personal data;

V - The regular exercise of rights in legal or administrative proceedings;

VI - The protection of the data subject's or a third party's life or physical safety;

VII - Health protection through a procedure performed by healthcare professional or the healthcare authorities.

§ 1 In the cases in which consent is not required, the data shall be processed exclusively for the purposes established and for the shortest period of time possible, in accordance with the general principles established in this Law and with respect to the data subject's rights.

§ 2 In the cases in which the provisions in sections I and II apply, said cases shall be publicly announced under the terms of paragraph 1 of Art. 6.

§ 3 In the event of breach of the provisions in section §2, the processor or controller for the data treatment may be held liable.

Section II

Sensitive Personal Data

Art. 12. The processing of sensitive personal data is forbidden, except:

I - If the data subject provides a special consent:

a) Through a specific statement, distinct from the consent pertaining to other personal data; and

b) If there is previous and specific information about the sensitive nature of the data to be processed, including a warning about the risks involved in the treatment of this type of data; or

II - Without the data subject's consent, in the case of unrestricted public access data, or if necessary to ensure:

a) The fulfilment of a legal obligation by the controller;

b) The processing and shared use of data pertaining to the exercise of rights or duties established in laws or regulation by the public authorities;

c) The performance of historical, scientific, or statistical research, ensuring, whenever possible, the dissociation of the personal data;

d) Regular exercise of rights in legal or administrative proceedings;

e) The protection of the data subject's or a third party's life or physical safety;

f) Health protection through a procedure performed by healthcare professional or the healthcare authorities.

§ 1 The provisions in this article apply to any processing that may disclose sensitive personal data.

§ 2 The processing of sensitive personal data must not be performed to the data subject's detriment, without prejudice to the provisions in specific legislation.

§ 3 In cases in which the provisions in items "a" and "b" are applied by public bodies and entities, said exemption from consent shall be publicly announced, according to section §1 of art. 6.

Art. 13. The competent body may establish additional measures for the security and protection of sensitive personal data, which shall be adopted by the controller or by other processing agents.

§ 1 The performance of certain types of processing of sensitive personal data may be subject to the previous consent by the competent body, under the terms of the regulations.

§ 2 The processing of biometric personal data shall be regulated by the competent body, which shall establish the cases in which biometric data shall be regarded as sensitive personal data.

Section III

Termination of the Processing

Art. 14. Processing of personal data shall be terminated in the following cases:

I - If it is verified that its purpose was achieved or that the data ceased to be necessary or relevant to achieve the specific purpose sought;

II - If the processing period ends;

III - At the data subject's request; or

IV - If the competent body establishes that the legislation or regulations were breached.

Sole paragraph. The competent body shall establish maximum periods for personal data processing, without prejudice to the provisions in the specific legislation.

Art. 15. The personal data shall be cancelled at the end of processing. They may be retained for the following purposes:

I - The fulfilment of a legal obligation by the controller;

II - The performance of historical, scientific, or statistical research, ensuring, whenever possible, the dissociation of the personal data;

III - Transfer to third parties under the terms of this Law.

Sole paragraph. The competent body may establish specific cases for the retention of personal data, ensuring the protection of the data subject's rights, without prejudice to the provisions in the specific legislation.

CHAPTER III

DATA SUBJECT'S RIGHTS

Art. 16. All natural persons are entitled to ownership of their personal data, and to the fundamental rights of freedom, intimacy and privacy, under the terms of this Law.

Art. 17. The personal data subject is entitled to obtaining:

I - The confirmation of the existence of data processing;

II - Access to the data;

III - The correction of incomplete, inaccurate, or outdated data; and

IV - The dissociation, blocking, or cancellation of unnecessary or excessive data, as well as of those data processed in non-compliance with the provisions in this Law.

§1 The data subject may object to the processing performed in one of the cases of exemption from consent on the basis of a breach of the provisions in this Law.

§ 2 The rights established in this article shall be exercised at the data subject's request to one of the processing agents, which shall immediately comply to the request.

§ 3 If it is impossible to immediately comply with the request as described in section §2, the controller shall send the data subject, within seven days from the date when the notification is received, an answer in which it may:

I - State that it is not a data processing agent; or

II - Specify the factual or legal reasons that prevent the immediate compliance with the request.

§ 4 Compliance with the request as set forth in section § 2 shall take place at no cost to the data subject.

§ 5 The controller shall notify the third parties to whom the data have been disclosed of the performance of any data correction, cancellation, dissociation, or blocking, so that they may repeat the same procedure.

Art. 18. The confirmation of the existence of or access to the personal data shall be provided, at the data subject's choice:

I - In simplified format, immediately; or

II - In a clear and full statement specifying the origin of the data, their registration data, the criteria used, and the purpose of the processing, provided within seven days from the data subject's request.

§ 1 Personal data shall be stored in a format that allows the exercise of right of access.

§ 2 The information may be provided, at the data subject's choice:

I - By electronic means which are safe and suitable for said purpose; or

II - In printed format, in which case only the cost of the services and materials used may be charged.

§ 3 The data subject may request a full electronic copy of their personal data in a format that allows their subsequent use, including in other processing operations, provided that the database is on an electronic support.

§ 4 The competent body may establish the formats in which the information and the data will be given to the data subject.

Art. 19. The data subject is entitled to request a review of decisions that are based on automated processing of personal data and that affect their interests only, including decisions aimed at defining their profile or evaluate aspects of their personality.

§ 1 The controller shall provide, whenever requested, adequate information about the criteria and procedures used for the automated decision.

§ 2 The processing of personal data required for compliance with legal obligations is exempted.

Art. 20. Personal data pertaining to regular exercise of rights by the data subject may not be used against the data subject.

Art. 21. The defence of data subjects' interests and rights may be exercised in an individual or collective legal proceeding, as established in Law No. 9,507 of 12 November 1997, Arts. 81 and 82

of Law No.-8,078 of 11 September 1990, in Law No. 7,347 of 24 July 1985, and other instruments for individual and collective protection.

CHAPTER IV

COMMUNICATION AND INTERCONNECTION

Art. 22. In cases of communication or interconnection of personal data, the transferee shall be subject to the same legal and regulatory obligations as the transferor, with which it shall be jointly liable for any damages caused.

Sole paragraph. Joint liability does not apply to cases of communication or interconnection performed in the exercise of the duties established in Law No. 12,527 of 18 November 2011 which regards to the guarantee of access to public information.

Art. 23. Communication or interconnection of personal data between private persons shall require free, express, specific, and informed consent, without prejudice to the cases of exemption from consent established in this Law.

Art. 24. Communication or interconnection of personal data between public and private persons shall require free, express, specific, and informed consent from the data subject, except:

I - In the cases of exemption from consent established in this Law;

II - In the cases of shared data use set forth in section XVII of art. 5, in which it shall be publicly announced under the terms of section §1 of art. 6; or

III - When previously authorised by the competent body, which shall assess the public interest, the suitability, and the need for the exemption from consent.

Sole paragraph. The consent established in section III of the main clause may be subject to:

I - the notification of the interconnection to the data subjects, under the terms of section §1 of Art. 6;

II - offering to the data subjects the possibility of cancellation of their data; or

III - compliance with complementary obligations established by the competent body.

Art. 25. Any communication or interconnection between public bodies and entities shall be publicly announced, under the terms of section §1 of art. 6, and shall follow the general rules established in this Chapter.

Art. 26. The competent body may request, at any time, to the public bodies and entities performing data interconnection and shared use of personal data, the provision of a specific report on the scope, nature of the data, and other details of the processing performed, and it may issue complementary recommendations to ensure compliance with this Law.

Art. 27. The competent body may establish complementary provisions for personal data communication and interconnection.

CHAPTER V

INTERNATIONAL DATA TRANSFER

Art. 28. International transfer of personal data is only allowed for countries that provide a level of protection for personal data that is equivalent to the level established in this Law, with no prejudice to the following exceptions:

I - When the transfer is necessary for international legal cooperation between public intelligence and investigation bodies, in accordance with instruments of international law;

II - When the transfer is necessary for the protection of the data subject's or a third party's life or physical safety;

III - When the competent body authorises the transfer under the terms of the regulations;

IV - When the transfer is the result of a commitment assumed in an international cooperation agreement;

V - When the transfer is necessary for the execution of a public policy or fall within a public service's legal powers, in which case it should be publicly announced under the terms of section §1 of art. 6.

Sole paragraph. A country's level of data protection shall be assessed by the competent body, which shall take into account:

I - The general and sectorial standards established in the country’s legislation;

II - The nature of the data;

III - Compliance with the general principles for personal data protection established in this Law;

IV - The adoption of security measures established in the regulations; and

V - Other specific factors pertaining to the transfer.

Art. 29. In the case of countries that do not provide a level of protection that is equivalent to that established in this Law, the consent described in Art. 7º shall be special, provided:

I - Through a specific statement, different from the consent pertaining to other processing operations; and

II - With prior and specific information about the international nature of the operation, including a warning about the risks involved, in accordance with the vulnerability circumstances of the destination country.

Art. 30. The authorisation mentioned in section III of the main clause of art. 28 shall be granted when the controller for the processing provides sufficient guarantees of compliance with the general principles of protection of the data subject's rights, presented in contractual clauses approved for a specific transfer, in standard contractual clauses, or in global corporate standards, under the terms of the regulations.

§ 1 The competent body may establish standard contractual clauses, which shall comply with the general principles of protection of the data subject's data and rights, ensuring the joint liability of the transferor and the transferee, regardless of fault.

§ 2 Any controllers and processors that are part of the same economic group or multinational conglomerate may submit global corporate rules for approval by the competent body, which shall be mandatory for all the companies in the group or conglomerate with no need for specific authorisations, subject to compliance with the general principles of protection and the data subject's rights.

§ 3 The analysis of contractual clauses or global corporate rules subject to approval by the competent body may require supplementary information requests or verification of the processing operations.

Art. 31. The transferor and the transferee shall be jointly liable for any data processing performed abroad or inside the national territory, in any case, regardless of fault.

Art. 32. In the event of an international data transfer from a foreign country to the national territory, processing in Brazil is only allowed when the operations performed in the foreign country have complied with its standards for obtaining consent.

Art. 33. The competent body may establish complementary rules for the identification of a processing operation such as an international personal data transfer.

CHAPTER VII

AGENTS' RESPONSIBILITY

Section I

Processing Agents and Damage Compensation

Art. 34. The personal data processing agents are the controller and the processor.

Art. 35. Any party that, through personal data processing, causes any individual or collective material or moral damage to another party shall be obligated to compensate the latter party.

§ 1 The judge in civil proceedings may place the burden of proof in favour of the data subject when, in in his discretion, the claim is likely to be true, or when the production of evidence by the data subject may be excessively burdensome;

§ 2 The controller or the processor may no longer be held liable if they can prove that the fact that caused the damage could not be attributed to them.

Art. 36. Potential exemption from consent does not exempt the agents from compliance with the other obligations established in this Law, in particularly compliance with the general principles and with guaranteeing the data subject's rights.

Art. 37. The penalties established under this Law shall be personally applied to any processors and controllers in public bodies that are non-compliant with this Law, according to the provisions of Law No. 8,112 of 11 December 1990 and Law No. 8,429 of 2 June 1992.

Art. 38. The competences and responsibilities pertaining to database management in public bodies and entities, as well as responsibility for the practice of administrative acts pertaining to personal data, shall be defined in the regulatory acts pertaining to the definition of their competences.

Section II

Controller and Processor

Art. 39. The processor shall perform the processing according to the instructions provided by the controller, who shall verify that the instructions and standards in this matter are complied with.

§ 1 The controller is jointly liable for all the processing operations performed by the processor.

§ 2 The competent body may request that the controller draft a report on the impact on privacy of its data processing operations, under the terms of the regulations.

Art. 40. The controller or the processor shall keep a record of the personal data processing operations performed, as established in art. 15.

Sole paragraph. The competent body may establish the format and structure of the record as well as how long it should be kept.

Section III

Person in Charge of Personal Data Processing

Art. 41. The controller shall appoint a person in charge of personal data processing.

§ 1 The identity and contact data of the person in charge shall be publicly disclosed in a clear and objective manner, preferably on the controller's website.

§ 2 The functions of the person in charge are:

I - To receive claims and communications from data subjects, provide clarification, and adopt measures;

II - To receive communications from the competent body and adopt measures;

III - To guide the entity’s employees regarding the practices to be followed pertaining to protection of personal data; and

IV - Other functions established in the complementary standards or by the controller.

§ 3 The competent body shall establish complementary rules on the definition and functions of the person in charge, including cases of exemption from the need for definition, according to the entity's nature or size, and the volume of its data processing operations.

Section IV

Data Security and Confidentiality

Art. 42. The processor shall adopt constantly updated technical and administrative measures, proportional to the nature of the information processed and suitable for protecting personal data from non-authorised access and from accidental or unlawful destruction, loss, change, communication, or disclosure, or any other form of unsuitable or unlawful processing.

Sole paragraph. The security measures must be compatible with the current state of technology, with the nature of the the data, and with the specific characteristics of the processing, in particular in the case of sensitive data.

Art. 43. the processors or any other person involved in any of the processing stages shall be bound by the duty of confidentiality regarding the personal data, even after the end of the processing.

Art. 44. The controller shall immediately report any security incident which might damage the data subjects to the competent body.

Sole paragraph. The notification shall include, at least:

I - A description of the nature of the personal data involved;

II - Information about the data subjects involved;

III - Specification of the security measures used for protection of the data, including any encryption procedures;

IV - Any related to the incident; and

V - Any measures adopted or to be adopted to reverse or mitigate the damaging effects

Art. 45. The competent body may adopt measures regarding security incidents involving personal data, depending on their seriousness, such as:

I - Prompt notification to data subjects;

II - Widespread dissemination of the fact in the media; or

III - Measures to reverse or mitigate the damaging effects.

§ 1 When assessing the seriousness of the incident, it will be verified if adequate technical measures were taken to make the personal data involved unintelligible for parties that are not authorised to access.

§ 2 Prompt notification to the data subjects affected by the security incident shall be mandatory, regardless of the competent body's decision, in cases in which the incident endangers the data subjects' personal safety or can damage them.

Art. 46. The systems used for personal data processing shall be structured so as to meet the security requirements, the general principles established in this Law, and the other regulatory rules.

Art. 47. The competent body may establish complementary rules concerning minimum criteria and standards of security, including those due to technological development.

Section V

Good Practice

Art. 48. The parties responsible for personal data processing, individually or by means of associations, may formulate good practice rules establishing conditions for organisation, operational system, procedures, security regulations, technical standards, specific obligations for the various parties involved in the processing, training actions, or internal oversight mechanisms, in compliance with the provisions in this Law and in complementary data protection statutes.

Sole paragraph. Good practice rules, made publicly available and update, may be recognised and disseminated by the competent body.

Art. 49. The competent body shall stimulate the adoption of technical standards for software and online applications that facilitate the availability of personal data to data subjects, including the right not to be monitored.

CHAPTER VIII

ADMINISTRATIVE PENALTIES

Art. 50. Any breaches of the standards established in this Law committed by private legal persons shall be subject to the following administrative penalties to be applied by the competent body:

I - A simple or daily fine;

II - The disclosure of the breach;

III - Dissociation of the personal data;

IV - Blocking of the personal data;

V - Suspension of the processing of personal data for a period no longer than two years;

VI - Cancellation of the personal data;

VII - Prohibition of the processing of sensitive personal data for a period no longer than ten years; and

VIII - Prohibition of database operation for a period no longer than ten years.

§ 1 Penalties may be cumulatively applied.

§ 2 The procedures and criteria for application of the penalties shall be adjusted to the severity and extent of the breach, the nature of the personal rights affected, the existence of a repeated offence, the infringing party's financial status, and the damage caused, under the terms of the regulations.

§ 3 The prohibition periods established in sections VII and VIII in the main clause may be extended by the competent body, if it is found that the relevant party's obligations have not been met, that the offence was repeated, or that compensation for the damages caused by the breach was not made in its entirety.

§ 4 The provisions established in this article shall not preclude the application of administrative, civil or criminal penalties defined in specific legislation.

§ 5 The provisions in sections III to VIII may be applied to public entities and bodies, without prejudice to the provisions in Law No. 8,112 of 11 December 1990 and in Law No. 8,429 of 1 June 1992.

CHAPTER IX

TEMPORARY AND FINAL PROVISIONS

Art. 51. The competent body shall establish gradual adaptation rules for databases created up to the date of entry into force of this Law, considering the complex nature of processing operations, the nature of the data, and the size of the controller.

Art. 52. This Law shall come into force within 120 (one hundred and twenty) days from its publication date.