The Congress of Colombia decrees:

Article 1. Purpose. The purpose of this law is to develop the constitutional right of individuals to know, update and correct any information referring to them, collected in data banks, and the other constitutional rights, freedoms and guarantees related to the gathering, treatment and circulation of personal data referred to in article 15 of the Political Constitution, as well as the right to information established in article 20 of the Political Constitution, particularly in relation to financial and credit, commercial and service information, as well as that obtained from third countries.

Article 2. Scope of application This law applies to any and all personal data kept in a data bank, whether managed by public or private entities.

This law shall apply, without prejudice to any special regulations stipulating the confidentiality of certain data or information kept in data banks of a public nature, for statistical purposes, investigation or sanctioning of crimes or to guarantee public order.

Excluded from this law are databases intended to build up State Intelligence by the Administrative Security Department, DAS, and the Public Forces, in order to guarantee internal and external national security.

Public records kept by chambers of commerce shall be governed exclusively by the rules and principles established in the special regulations that apply to them.

Similarly, any data kept within an exclusively personal or domestic environment and those which circulate internally, that is, which are not provided to other individuals or legal entities, are excluded from the application of this law.

Article 3. Definitions. The following definitions shall apply for the purposes of this law:

a) Data subject. Is the individual or legal entity to which the information kept in a data bank refers and is the object of the right of *habeas data* and other rights and guarantees referred to in this law;

b) Source of information. Is the person, entity or organization which receives or knows personal information of the data subjects, by virtue of a commercial or service relationship or otherwise and which, pursuant to a legal authorization or one given by the data subject, provides such data to an information operator, which shall in turn deliver it to the end user. If the source delivers the information directly, and not through an operator, to the users, it shall have the double status of source and operator and shall take on the duties and responsibilities of both. The source of the information is responsible for the quality of the data supplied to the operator and, when it has access to and supplies personal information of third parties, is subject to compliance with the duties and responsibilities provided to ensure the protection of the rights of the data subject;

c) Information operator. The information operator is the person, entity or organization that receives from the source personal data regarding several data subjects, manages it and transmits it to the users under the parameters of this law. Therefore, the operator, to the extent that it has access to third party personal information, is subject to compliance with the duties and responsibilities provided to ensure the protection of the rights of the data subject. Unless the operator is also the source of the information, it has no commercial or service relationship with the data subject and therefore is not responsible for the quality of the data provided to it by the source;

d) User. The user is the individual or legal entity which, in the terms and circumstances provided in this law, may access personal information of one or several data subjects provided by the operator or by the source, or directly by the data subject. To the extent that the user has access to third party personal information, it must comply with the duties and responsibilities provided to ensure the protection of the rights of the data subject. In case the user in turn delivers the

information directly to an operator, it shall have the double status of user and source, and shall take on the duties and responsibilities of both;

e) Personal data. Is any piece of information related to one or several specific or specifiable persons or which can be associated with an individual or legal entity. Impersonal data are not subject to the data protection regime of this law. When this law contains a reference to data, it is presumed to be data of personal use. Personal data may be public, semi-private or private;

f) Public data. Are the data classified as such according to the mandates of the law or the Political Constitution and all those which are not semi-private or private, in accordance with this law. Public data are, among others, those contained in public documents, duly executed legal judgments which are not privileged and those related to the marital status of individuals;

g) Semi-private data. Semi-private data are those which are not of a private, confidential or public nature, the knowledge or disclosure of which might interest not only their subject but also a certain sector or group of individuals or society in general, such as the financial or credit, commercial or service activity data referred to in Title IV of this law.

h) Private data. Are the data which due to their private or confidential nature are relevant only to their data subject.

i) Commercial Information Bureau. Is any legally organized company whose main activity is the collection, validation and processing of commercial information on companies and merchants specifically requested by its clients, commercial information being understood as any historical and current information related to the financial standing, equity, market, administrative or operating situation, fulfillment of obligations and other relevant information to analyze the integral situation of a company. For the purposes of this law, commercial information bureaus are information operators and information sources.

Paragraph: The following provisions of this law shall not apply to commercial information bureaus, or to their sources or users, as the case may be: Numerals 2 and 6 of article 8, article 12, and article 14.

j) Financial, credit, commercial or service information and that obtained from third countries.

For all purposes of this law, financial, credit, commercial or service information and that obtained from third countries shall be understood to be that referring to the creation, performance and extinguishment of monetary obligations, regardless of the nature of the contract from which they originated, as well as information related to the other activities pertaining to the financial sector or regarding the financial management or financial statements of the data subject.

Article 4. Principles of data administration. The principles established below shall be taken into account in the development, interpretation and application of this law, in a harmonious and integral manner:

a) Principle of veracity or quality of the records or data. The information contained in data banks must be truthful, complete, accurate, current, verifiable and clear. The recording and disclosure of partial, incomplete or fractioned data, or data which may lead to error, is prohibited;

b) Principle of purpose. The administration of personal data must have a legitimate purpose according to the Constitution and the law. The purpose must be informed to the data subject prior to or concomitantly with the granting of the authorization, when it is necessary or in general, provided the data subject requests information in this respect:

c) Principle of restricted circulation. The administration of personal data is subject to the limitations that derive from the nature of the data, from the provisions of this law and from the principles of

personal data administration, particularly the principles of transience of the information and the purpose of the data bank.

Personal data, except for public information, may not be accessible via the Internet or through other means of disclosure or mass communication, unless access thereto is technically controllable in order to provide restricted knowledge thereof only to the data subjects or users authorized in accordance with this law;

d) Principle of transience of information. The information of the data subject may not be provided to users or third parties when it ceases to serve the purpose of the data bank;

e) Principle of integral interpretation of constitutional rights. This law shall be interpreted so as to properly protect constitutional rights, such as *habeas data*, the right to a good name, the right to honor, the right to privacy and the right to information. The rights of data subjects shall be interpreted in harmony and in a balanced plane with the right to information contemplated in article 20 of the Constitution and with the other applicable constitutional rights;

f) Principle of security. The information included in the individual records making up the data banks referred to in the law, as well as that resulting from consultations by their users, must be handled with the technical measures that may be necessary to guarantee the security of the records avoiding their falsification, loss, unauthorized consultation or use;

g) Principle of confidentiality. Any individuals or legal entities involved in the administration of personal data which are not of a public nature are under the obligation to guarantee at all times the confidentiality of the information, even after the end of their relationship with any of the tasks comprising data administration, being able to take part in the provision or communication of data when this corresponds to the performance of the activities authorized in this law and in the terms hereof.

Article 5. Circulation of information. The personal information collected or provided as established by law to the operators, which is part of the managed data bank, may be provided orally, in writing, or placed at the disposal of the following individuals and in the following terms:

a) To the data subjects, to the persons duly authorized by these and to their assignees through the consultation procedure provided in this law.

b) To the users of the information, within the parameters of this law.

c) To any judicial authority, upon a prior court order.

d) To the public entities of the executive branch of Government, when the knowledge of said information related directly to the performance of any of their functions.

e) To the control bodies and other bodies engaged in disciplinary, fiscal or administrative investigation, when the information is necessary for the development of an investigation in progress.

f) To other data operators, with the authorization of the data subject, or when without requiring the authorization of the data subject the destination data bank has the same purpose or a purpose comprising that of the operator delivering the data. If the receiver of the information were a foreign data bank, the delivery without authorization of the data subject may only be made leaving written evidence of the delivery of the information and upon prior verification by the operator that the laws of the respective country or the receiver provide sufficient guarantees for the protection of the rights of the data subject.

g) To other persons authorized by law.

TITLE II
RIGHTS OF THE DATA SUBJECTS.

Article 6. Rights of the data subjects. The data subjects shall have the following rights:

1. With respect to data bank operators:

1.1 To exercise the fundamental right to *habeas data* upon the terms of this law, through the use of the consultation or claim procedures, without prejudice to the other constitutional and legal mechanisms.

1.2 To demand respect for and protection of the other constitutional or legal rights, as well as of the other provisions of this law, through the use of the claims and petitions procedure.

1.3 To request proof of the certification of existence of the authorization issued by the source or by the user.

1.4 To request information about the users authorized to obtain information.
Paragraph. The administration of public information does not require authorization of the data subject, but it is subject to compliance with the principles of personal data administration and the other provisions of this law.

The administration of semi-private and private data requires the prior and express consent of the data subject, except in the case of financial, credit, commercial and service data and those obtained from third countries, which does not require such authorization. In any event, the administration of semi-private and private data is subject to compliance with the principles of personal data administration and to the other provisions of this law.

2. With respect to the sources of the information:

2.1 To exercise the fundamental rights to *habeas data* and petition, which may be complied with through the operators, as provided in the consultation and claim procedures of this law, without prejudice to the other constitutional or legal mechanisms.

2.2 To request information or demand the update or correction of data contained in the database, which shall be done by the operator, based on the information provided by the source, as established in the procedure for consultations, claims and petitions.

2.3 To request proof of the authorization, when said authorization is required as provided in this law.

3. With respect to the users:

3.1 To request information on the use that the user is making of the information, when said information has not been provided by the operator.

3.2 To request proof of the authorization, when it is required as provided in this law.

Paragraph. Financial and credit data subjects shall additionally have the following rights:

They may go to the surveillance authority to file complaints against the sources, operators or users for violation of the rules on administration of financial and credit information.

In addition, they may go before the surveillance authority to demand that an operator or source be ordered to correct or update their personal data, when appropriate as established in this law.

TITLE III
DUTIES OF THE OPERATORS, SOURCES AND USERS OF INFORMATION

Article 7. Duties of the data bank operators. Without prejudice to their compliance with the other provisions contained in this law and others governing their activity, data bank operators are required to:

1. Guarantee, at all times, to the data subject, the full and effective exercise of the rights of *habeas data* and petition, that is, the possibility of knowing the information related to it that exists or is kept in the data bank, and requesting the update or correction of data, all of which must be done through the consultation or claim mechanisms, as provided in this law.

2. Guarantee that in the collection, treatment and circulation of data, they will respect the other rights established in the law.

3. Permit access to the information only to those persons who, in accordance with this law, are allowed such access.

4. Adopt an internal policies and procedures manual to guarantee proper compliance with this law and, in particular, for the handling of consultations and claims by the data subjects.

5. Request certification from the source regarding the existence of the authorization granted by the data subject, whenever said authorization is necessary, as provided in this law.

6. Retain, with the proper security measures, the records stored in order to prevent their deterioration, loss, alteration, unauthorized or fraudulent use.

7. Carry out a periodic and timely update and correction of the data, whenever the sources report recent changes, according to the terms of this law.

8. Process the petitions, consultations and claims made by the data subjects, according to the terms of this law.

9. Indicate in the respective individual record that certain information is under discussion by its subject, when a request for correction or update of same has been filed and said process has not ended, in the manner regulated in this law.

10. Circulate the information to the users, within the parameters of this law.

11. Comply with the instructions and requirements issued by the surveillance authority in relation to compliance with this law.

12. Any others derived from the Constitution or from this law.

Article 8. Duties of the sources of information. The sources of information must fulfill the following obligations, without prejudice to their compliance with the other provisions set out in this law and in others governing their activity:

1. Ensure that the information provided to data bank operators or users is truthful, complete, accurate, current and verifiable.

2. Report to the operator, in a periodic and timely manner, any recent changes with respect to previously furnished data and take any other steps that may be necessary in order for the information provided to be kept current.

3. Rectify the information when it is incorrect and inform the operators as appropriate.

4. Design and implement effective mechanisms to report the information promptly to the operator.

5. Request, when such is the case, and retain a copy or evidence of the respective authorization given by the data subjects, and make sure not to disclose to the operators any data whose disclosure has not been previously authorized, when said authorization is necessary, as provided in this law.

6. Certify semi-annually to the operator that the information provided has the authorization required under this law.

7. Resolve the claims and petitions of data subjects in the manner regulated in this law.

8. Inform the operator that certain information is being disputed by the data subject, when a request for correction or update of same has been filed, in order for the operator to include a note in the data bank to that effect until the process has ended.

9. Carry out the instructions issued by the control authority in relation to compliance with this law.

10. Any others derived from the Constitution or this law.

Article 9. Duties of the users. Without prejudice to their compliance with the regulations contained in this law and others governing their activity, users of the information must:

1. Keep confidential the information provided to them by data bank operators, sources or data subjects and use the information only for the purposes for which it was furnished, according to the terms of this law.

2. Inform the data subjects, at their request, regarding the use that is being made of the information.

3. Preserve, with the proper security measures, the information received, in order to prevent its deterioration, loss, alteration, unauthorized or fraudulent use.

4. Follow the instructions issued by the control authority in relation to compliance with this law.

5. Any others derived from the Constitution or this law.

TITLE IV
ON DATA BANKS FOR FINANCIAL, CREDIT, COMMERCIAL AND SERVICE INFORMATION AND THAT OBTAINED FROM THIRD COUNTRIES.

Article 10. Principle of favoring a public interest activity. The administration of financial, credit, commercial and service information, and that obtained from third countries, is directly related to and favors a public interest activity, such as financial activity itself, as it aids the democratization of credit, promotes the development of credit activity, the protection of public confidence in the financial system and the stability of same, and generates other benefits for the domestic economy and in particular for the financial, credit, commercial and service activity of the country.

Paragraph 1. The administration of financial, credit, commercial and service information and that obtained from third countries, by sources, users and operators, must be carried out so as to promote the expansion and democratization of credit. Users of this type of information must assess it concurrently with other factors or elements of judgment which technically impact risk

studies and credit analyses, and may not be based exclusively on information related to the non-performance of obligations provided by the operators in order to make decisions regarding credit requests.

The Colombian Financial Superintendency may impose the penalties provided in this law on users of the information who deny a credit application based exclusively on the applicant's negative information report.

Paragraph 2. The financial, credit, commercial and service information, and that obtained from third countries, may be consulted by the data subject free of charge at least once during each calendar month.

Article 11. Special requirements for operators. Operators of data banks containing financial, credit, commercial and service information, and that obtained from third countries, which operate as independent entities from the sources of the information, must meet the following special operating requirements:

1. They must be organized as commercial companies, non-profit institutions or cooperative entities.

2. They must have a service area for data subjects, in order to handle petitions, consultations and claims.

3. They must have a security system and other technical conditions, sufficient to guarantee the security and update of the records, preventing their falsification, loss, unauthorized consultation or use, as provided in this law.

4. They must update the information reported by the sources at least every ten (10) calendar days counted as of the receipt of same.

Article 12. Special requirements for sources. The sources must update, on a monthly basis, the information provided to the operator, without prejudice to what is provided in Title III of this law.

Negative information reports on the nonperformance of obligations of any nature, provided by sources of information to the operators of financial, credit, commercial and services information as well as that obtained from third countries, will only be admissible upon prior communication to the data subject, in order to allow the latter to demonstrate or effect payment of the obligation, as well as argue aspects such as the amount of the obligation or installment and its due date. Said communication may be included in the periodic statements sent by the sources of information to their clients.

In any event, sources of information may issue the information report twenty (20) calendar days after the date on which the communication has been sent to the last address of the affected party registered in the files of the source and without prejudice, if such were the case, to their compliance with the obligation to inform the operator that the information is under debate by its subject, when a request for correction or update has been filed and not resolved yet.

Article 13. Retention of the information. Positive information will remain indefinitely in the data banks of the information operators.

Data whose content refers to the time of delay, type of collection, portfolio status and, in general, any data referring to a situation involving a default of obligations, shall be subject to a maximum retention term, after which it must be removed from the data banks by the operator, in such a way that users cannot access or consult said information. The retention term of this information shall

be four (4) years counted as of the date on which any pending installments or overdue obligations are paid.

Article 14. Content of the information. The National Government shall determine the manner in which data banks holding financial, credit, commercial and service information, and that obtained from third countries, must present the information related to the data subjects. To that end, it shall establish a form that permits the identification, among other aspects, of the full name of the debtor, the capacity in which he or she is acting, that is, as principal debtor, joint and several debtor, guarantor or surety, the amount of the overdue obligation or installment, the time of delay and the date of payment, if such were the case.

In exercising the power granted in the previous paragraph, the National Government must take into account that in the report form it must establish that:

a) A negative report is presented when the individual(s) or legal entity(ies) are effectively behind in the payment of their installments or obligations.

b) A positive report is presented when the individual(s) and legal entity(ies) are current in their obligations.

A failure to comply with the obligation established herein shall result in the imposition of the maximum penalties contemplated in this law.

Paragraph 1. For the purposes of this law, it is understood that an obligation has been voluntarily paid when its payment has occurred without the intervention of a legal judgment ordering so.

Paragraph 2. The consequences established in this article for the voluntary payment of overdue obligations shall apply to any other mode of extinguishment of obligations, which is not the result of a legal judgment.

Paragraph 3. When a user consults the status of a data subject in databases containing financial, credit, commercial and service information, as well as that obtained from third countries, these must provide accurate information on its current status, that is, issue a positive report for users which at the time of the consultation are up-to-date in their obligations and a negative report for those which at the time of the consultation are in default with respect to an installment or obligation.

The remaining information contained in financial, credit, commercial and services databases, as well as that obtained from third countries, will be part of the credit history of each user, which may be consulted by the user, provided it has been informed of the current status.

Paragraph 4. The administration of personal data with exclusively unfavorable information is prohibited.

Article 15. Access to information by users. The information contained data banks with financial, credit, commercial and services information, as well as that obtained from third countries, may be accessed by users only for the following purposes:

As an element of analysis to establish and maintain a contractual relationship, regardless of its nature, as well as to assess the risks related to a current contractual relationship.

As an element of analysis to conduct market studies or commercial or statistical research.

In order to conduct any proceedings before a public authority or a private person, in respect of which said information is pertinent.

For any purpose other than the foregoing, in respect of which and in a general manner or for each particular case, authorization has been obtained from the data subject.

TITLE V
CONSULTATION REQUESTS AND CLAIMS

Article 16. Petitions, Consultations and Claims.

I. Processing of consultations. Data subjects or their assignees may consult the personal information of the data subject, kept in any data bank, whether of the public or private sector. The operator must provide these, once they have duly identified themselves, with all information contained in the individual record or related to the data subject's identification.

The petition or consultation of information shall be made orally, in writing, or by any means of communication, provided evidence of the consultation is kept using technical means.

The petition or consultation shall be answered within a maximum term of ten (10) business days counted as of the date of its receipt. When it is not possible to respond to the petition or consultation within said term, the interested party must be informed accordingly, stating the reasons for the delay and indicating the date when the petition will be answered, which may not exceed, under any circumstances, five (5) business days following the expiration of the first term.

Paragraph. The petition or consultation must be attended to thoroughly, fully providing any information requested.

II. Processing of claims. Data subjects or their assignees who feel that the information contained in their individual record in a data bank should be corrected or updated may file a claim with the operator, which shall be processed according to the following rules:

1. The petition or claim must be made in writing, addressed to the data bank operator, including the identification of the data subject, a description of the facts behind the claim, the address, and if such were the case, accompanied by the supporting documents that are to be used. In case the writing is incomplete, an official communication must be sent to the interested party to remedy any faults. If one month after the date of the request the applicant has not submitted the required information, it shall be understood that he or she has abandoned the claim or petition.

2. Once the complete petition or claim has been received, the operator will include in the individual record, within a term of no more than two (2) business days, a note stating “claim in process” and the nature thereof. Said information must be maintained until the claim has been decided and must be included in any information provided to users.

3. The maximum term to answer a petition or claim shall be fifteen (15) business days counted as of the day following the date of its receipt. When it is not possible to respond to the petition within said term, the interested party shall be informed accordingly, stating the reasons for the delay and indicating the date when the petition will be answered, which may not exceed, under any circumstances, eight (8) business days following the expiration of the first term.

4. In cases where there is a source of information that is independent from the operator, the latter must notify the claim to the source within a maximum term of two (2) business days, and the source must resolve it and reply to the operator within a maximum term of ten (10) business days. In any event, the answer must be provided to the data subject by the operator within a maximum term of fifteen (15) business days counted as of the day following the filing date of the claim, which term may be extended for an additional eight (8) business days, as indicated in the previous section. If the claim is filed with the source, it shall proceed to resolve the claim directly, but must inform the operator regarding its receipt of the claim within two (2) business days following said

receipt, in such a way that the obligation to include the note stating “claim in process” as well as the nature of same in the individual record can be complied with, which must be done by the operator within two (2) business days following that on which the information has been received from the source.

5. In order to reply to a petition or claim, the operator or source, as the case may be, must carry out a full verification of the observations or arguments of the data subject, making sure that it reviews any pertinent information in order to provide a complete answer to the data subject.

6. Without prejudice to the exercise of a *tutela* action to protect the fundamental right of *habeas data*, in case the data subject is not satisfied with the answer to the petition, he may resort to the appropriate judicial proceeding within the pertinent legal terms in order to debate any aspect related to the obligation reported as not performed. The complaint must ser filed against the source of the information which, once notified of same, shall proceed to inform the operator within the next two (2) business days, in such a way that the obligation to include the note stating “information under judicial dispute” and the nature of same within the individual record can be complied with, which the operator must do within two (2) business days following that on which it received the information from the source and for the entire time it takes to obtain a final decision. The same procedure must be followed in case the source files a judicial proceeding against the data subject, regarding the obligation reported as not performed, and the latter proposes defenses on the merits.

TITLE VI
SURVEILLANCE OF ENTITIES COVERED BY THE LAW

Article 17. Surveillance function. The Superintendency of Industry and Commerce shall exercise the surveillance of the operators, sources and users of financial, credit, commercial and service information and that obtained from third countries, with respect to the personal data administration activity regulated in this law.

In those cases where the source, user or operator of the information is an entity supervised by the Colombian Financial Superintendency, the latter shall exercise the surveillance and impose the relevant penalties, in accordance with the powers pertaining to it, as established in the Organic Law of the Financial System and the other pertinent regulations, as well as those established in this law.

In order to exercise the surveillance function referred to in this article, the Superintendency of Industry and Commerce and the Colombian Financial Superintendency, as the case may be, shall have, in addition to their own, the following powers:

1. Issue instructions and orders regarding the manner in which the provisions of this law related to the administration of financial, credit, commercial and service information, and that obtained from third countries, must be complied with and establish the criteria to facilitate their performance and determine procedures for their prompt application.

2. See to compliance with the provisions of this law, with the rules regulating it and the instructions issued by the respective Superintendency.

3. Verify that the operators and sources have a security system and other technical conditions sufficient to guarantee the security and update of the records, preventing their falsification, loss, unauthorized consultation or use, as provided in this law.

4. Order, for account of the operator, the source or the user, the performance of external systems audits to verify compliance with the provisions of this law.

5. Order *sua sponte* or at the request of a party, the correction, update or removal of personal data, when appropriate, as established in this law. When this is done at the request of the a party, evidence must be provided to the Superintendency to demonstrate that a claim based on the same facts was processed before the operator or the source, and that it was not responded to or was unfavorably resolved.

6. Initiate *sua sponte* or at the request of a party, administrative investigations against the operators, sources and users of financial, credit, commercial and service information and that obtained from third countries, in order to determine whether there is administrative liability derived from nonobservance of the provisions of this law or of the orders or instructions issued by the respective surveillance entity, and if such were the case, impose penalties or order the measures that may be pertinent.

Article 18. Penalties. The Superintendency of Industry and Commerce and the Financial Superintendency may impose on the operators, sources or users of financial, credit, commercial or service information, and that obtained from third countries, providing the pertinent explanations according to the applicable procedure, the following penalties:

Fines of a personal and institutional nature for up to the equivalent of one thousand five hundred (1,500) current minimum monthly legal wages at the time of imposition of the penalty, due to the violation of this law or the rules regulating it, as well as for the nonobservance of the orders and instructions imparted by said Superintendency. The fines established herein may be successive for as long as the nonperformance that originated them subsists.

Suspension of activities of the data bank, for up to a term of six (6) months, when the information is being managed in a way that seriously infringes the conditions and requirements established in this law, as well as due to the nonobservance of the orders and instructions given by the mentioned Superintendencies in order to correct said infringements.

Closing of the data bank's operations when, once the term of suspension has elapsed, it has not adjusted its technical and logistic operation, and its regulations and procedures, to the legal requirements, as provided in the resolution that ordered the suspension.

Immediate and final closing of the operation of data banks that handle prohibited data.

Article 19. Criteria to determine penalties. The penalties for infringements referred to in the previous article will be determined according to the following criteria, to the extent applicable:

a) The extent of the damage or danger to the legal interests protected by this law.

b) The economic benefit obtained by the infringer or by third parties, by committing the infringement, or the damage that said infringement may have caused.

c) The repetition of the infringement.

d) The opposition, refusal or obstruction of the investigation or surveillance action of the Superintendency of Industry and Commerce.

e) The unwillingness or refusal to comply with the orders given by the Superintendency of Industry and Commerce.

f) The express recognition or acceptance by the investigated party of the commission of the infringement before the imposition of the relevant penalty.

Article 20. Transition system for Control Entities. The Superintendent of Industry and Commerce and the Financial Superintendent shall take on the functions established herein, six (6)

months after the effectiveness of this law. For such purpose, the National Government shall take, within said term, the necessary steps to adjust the structure of the Industry, Commerce and Financial Superintendency, providing them with the necessary budgetary and technical capacity to perform said functions.

TITLE VII
FINAL PROVISIONS

Article 21. Transition system. To comply with the provisions contained in this law, the persons who, as of its effective date, are exercising any of the activities regulated herein, shall have a term of up to six (6) months to adjust their operation to the regulations of this law.

Data subjects who, as of the effectiveness of this law, are up-to-date in the obligations object of the report, and whose negative information has remained in the data banks at least a year counted as of the settlement of those obligations, shall benefit from the immediate lapsing of the negative information.

In turn, data subjects who are up-to-date in their obligations object of the report, but whose negative information has not remained in the data banks at least one year after the settlement of their obligations, shall remain with said negative information for the time remaining to complete one year, counted as of the settlement of the obligations.

Data subjects who repay the obligations subject to reporting within six (6) months following the effectiveness of this law, shall remain with said negative information in the data banks for a term of one (1) year, counted as of the settlement date of said obligations. Once this term of one (1) year has ended, the negative data must be automatically removed from the data banks.

The benefit provided in this article will be lost in case the data subject incurs a new default, in which case its report shall again reflect all past defaults, upon the terms provided in article 13 of this law.

Article 22. Effectiveness and repeals. This law shall take effect as of its date of publication and revokes all regulations that may be contrary to it.