



Law 1581 of 2012

Download PDF

Dates



Topics (3)



Validity(3)

Regulated by Decree 1081 of 2015 Sector Presidency of the Republic

Regulated by Decree 886 of 2014

Regulated by Decree 1377 of 2013

The published data is for informational purposes only. The Administrative Department of Public Service is not responsible for the current validity of this regulation. We are in a continuous process of updating the content.

STATUTORY LAW 1581 OF 2012

(October 17)

[Partially regulated by National Decree 1377 of 2013](#) , [Partially regulated by Decree 1081 of 2015](#). See ruling [C-748 of 2011](#). See [Decree 255 of 2022](#).

Which establishes general provisions for the protection of personal data.

THE CONGRESS OF COLOMBIA

DECREES:

TITLE I

OBJECT, SCOPE AND DEFINITIONS

Article 1. Purpose . The purpose of this law is to develop the constitutional right of all persons to know, update and rectify the information that has been collected about them in databases or files, and the other constitutional rights, freedoms and guarantees referred to in Article [15](#) of the Political Constitution; as well as the right to information enshrined in Article 20 of the same.

Article2. Scope of application . The principles and provisions contained in this law shall apply to personal data recorded in any database that makes them susceptible to processing by entities of a public or private nature .

This law will apply to the processing of personal data carried out in Colombian territory or when the Data Controller or Data Processor not established in the national territory is subject to Colombian legislation by virtue of international norms and treaties.

The personal data protection regime established in this law shall not apply:

a) To databases or files maintained in an exclusively personal or domestic context.

When these databases or files are to be provided to third parties, the Data Subject must be informed beforehand and their authorization requested. In this case, the Data Controllers and Processors of the databases and files will be subject to the provisions contained in this law;

b) To databases and files whose purpose is national security and defense, as well as the prevention, detection, monitoring and control of money laundering and the financing of terrorism;

c) To databases whose purpose is and which contain intelligence and counterintelligence information;

d) To databases and archives of journalistic information and other editorial content;

e) To the databases and files regulated by Law [1266](#) of 2008;

f) To the databases and files regulated by Law [79](#) of 1993.

Paragraph. The principles on data protection shall apply to all databases, including those excepted in this article, within the limits established by this law and without prejudice to data that is protected by legal confidentiality. If the special regulations governing the excepted databases provide for principles that take into account the special nature of the data, those principles shall apply concurrently with those provided for in this law.

Article3. Definitions . For the purposes of this law, **the** following definitions apply:

a) **Authorization:** Prior, express and informed consent of the Holder to carry out the Processing of personal data;

b) **Database:** An organized set of personal data that is subject to processing;

c) **Personal data:** Any information linked to or that can be associated with one or more specific or identifiable natural persons;

d) **Processor:** Natural or legal person, public or private, who, alone or in association with others, carries out the processing of personal data on behalf of the Data Controller;

e) **Data Controller:** Natural or legal person, public or private, who alone or jointly with others, decides on the database and/or the processing of the data;

f) **Data Subject** : Natural person whose personal data is subject to Processing;

g) **Processing:** Any operation or set of operations performed on personal data, such as collection, storage, use, circulation or deletion.

TITLE II

GUIDING PRINCIPLES

Article4. Principles *for the Processing of Personal Data.*

In the development, interpretation and application of this law, the following principles shall be applied in a harmonious and comprehensive manner:

- a) **Principle of legality in matters of data processing:** The processing referred to in this law is a regulated activity that must comply with the provisions of this law and other regulations that develop it;
- b) **Principle of purpose:** The Processing must obey a legitimate purpose in accordance with the Constitution and the Law, which must be informed to the Data Subject;
- c) **Principle of freedom:** Processing may only be carried out with the prior, express and informed consent of the Data Subject. Personal data may not be obtained or disclosed without prior authorization, or in the absence of a legal or judicial mandate that waives the requirement for consent;
- d) **Principle of truthfulness or quality:** The information subject to Processing must be truthful, complete, accurate, up-to-date, verifiable and understandable. The Processing of partial, incomplete, fragmented or misleading data is prohibited;
- e) **Principle of transparency:** In the Processing, the right of the Data Subject to obtain from the Controller or the Processor, at any time and without restrictions, information about the existence of data concerning him or her must be guaranteed;
- f) **Principle of restricted access and circulation:** The Processing is subject to the limits derived from the nature of the personal data, the provisions of this law and the Constitution. In this sense, the Processing may only be carried out by persons authorized by the Data Subject and/or by the persons provided for in this law;

Personal data, except for public information, may not be available on the Internet or other means of mass dissemination or communication, unless access is technically controllable to provide restricted knowledge only to the Data Subjects or authorized third parties in accordance with this law;

g) **Security Principle:** The information subject to Processing by the Data Controller or Data Processor referred to in this law, must be handled with the technical, human and administrative measures that are necessary to provide security to the records, preventing their alteration, loss, consultation, use or unauthorized or fraudulent access;

h) **Principle of confidentiality:** All persons involved in the processing of personal data that are not of a public nature are obliged to guarantee the confidentiality of the information, even after their relationship with any of the tasks that comprise the processing has ended, and may only supply or communicate personal data when it corresponds to the development of the activities authorized in this law and in accordance with its terms.

TITLE III

SPECIAL DATA CATEGORIES

Article5. Sensitive Data . For the purposes of this law, sensitive data is understood to be data that affects the privacy of the Data Subject or whose misuse may generate discrimination, such as data that **reveals** racial or ethnic origin, political orientation, religious or philosophical beliefs, membership in trade unions, social or human rights organizations or organizations that promote the interests of any political party or that guarantee the rights and guarantees of opposition political parties, as well as data relating to health, sex life and biometric data.

Article6. Processing of sensitive data. The processing of sensitive data is prohibited, except when:

- a) The Data Subject has given explicit authorization to said Processing, except in cases where the granting of such authorization is not required by law;
- b) The processing is necessary to safeguard the vital interests of the data subject and the data subject is physically or legally incapable of giving consent. In these cases, the legal representatives must give their authorization;

- c) The processing is carried out in the course of legitimate activities and with appropriate safeguards by a foundation, NGO, association or any other non-profit organization whose purpose is political, philosophical, religious or trade union-related, provided that it relates exclusively to its members or to persons who maintain regular contact with it in connection with its purpose. In these cases, the data may not be provided to third parties without the data subject's authorization;
- d) The processing refers to data that is necessary for the recognition, exercise or defense of a right in a judicial process;
- e) The processing has a historical, statistical, or scientific purpose. In this case, measures must be taken to suppress the identity of the data subjects.

Article 7. *Rights of children and adolescents.*

The Treatment will ensure respect for the prevailing rights of children and adolescents.

The processing of personal data of children and adolescents is prohibited, except for data that is of a public nature.

It is the responsibility of the State and educational institutions of all types to provide information and training to legal representatives and guardians regarding the potential risks faced by children and adolescents concerning the improper handling of their personal data, and to provide them with knowledge about the responsible and safe use of their personal data, their right to privacy and the protection of their personal information and that of others. The National Government will regulate this matter within six (6) months following the enactment of this law.

TITLE IV

RIGHTS AND LEGAL CONDITIONS FOR DATA PROCESSING

Article 8. *Rights of Data Subjects.* The Data Subject shall have the following rights:

- a) To know, update and rectify your personal data before the Data Controllers or Data Processors. This right may be exercised, among others, with respect to partial, inaccurate, incomplete, fragmented, misleading data, or data whose processing is expressly prohibited or has not been authorized;
- b) Request proof of the authorization granted to the Data Controller except when expressly exempted as a requirement for the Processing, in accordance with the provisions of Article 10 of this law;
- c) To be informed by the Data Controller or the Data Processor, upon request, regarding the use that has been made of your personal data;
- d) To file complaints with the Superintendency of Industry and Commerce for violations of the provisions of this law and other regulations that modify, add to or complement it;
- e) Revoke authorization and/or request the deletion of data when the Processing does not respect constitutional and legal principles, rights, and guarantees. Revocation and/or deletion will proceed when the Superintendency of Industry and Commerce has determined that the Controller or Processor has engaged in conduct contrary to this law and the Constitution;
- f) Access free of charge to your personal data that has been processed.

Article 9. *Data Subject's Authorization.* Without prejudice to the exceptions provided for by law, the Processing requires the prior and informed authorization of the Data Subject, which must be obtained by any means that can be subsequently consulted.

Article 10. *Cases in which authorization is not required.* The Holder's authorization will not be required when it involves:

- a) Information required by a public or administrative entity in the exercise of its legal functions or by court order;
- b) Data of a public nature;

- c) Cases of medical or health emergency;
- d) Processing of information authorized by law for historical, statistical or scientific purposes;
- e) Data related to the Civil Registry of Persons.

Anyone who accesses personal data without prior authorization must in all cases comply with the provisions contained in this law.

Article 11. *Provision of Information* . The requested information may be provided by any means, including electronic means, as required by the Data Subject. The information must be easily readable, without technical barriers that impede access, and must correspond in its entirety to that contained in the database.

The National Government will establish the manner in which the Data Controllers and Data Processors must provide the information of the Data Subject, taking into account the nature of the personal data. This regulation must be issued no later than one year after the promulgation of this law.

Article 12. *Duty to inform the Data Subject*. When requesting authorization from the Data Subject, the Data Controller must clearly and expressly inform them of the following:

- a) The treatment to which your personal data will be subjected and the purpose thereof;
- b) The optional nature of the response to the questions asked, when these relate to sensitive data or to the data of girls, boys and adolescents;
- c) The rights that you have as the Holder;
- d) The identification, physical or electronic address and telephone number of the Data Controller.

Paragraph. The Data Controller shall keep proof of compliance with the provisions of this article and, when requested by the Data Subject, provide him with a copy thereof.

Article 13. *Persons to whom information may be provided* . Information that meets the conditions established in this law may be provided to the following persons:

- a) To the Holders, their successors or their legal representatives;
- b) To public or administrative entities in the exercise of their legal functions or by judicial order;
- c) To third parties authorized by the Owner or by law.

TITLE V

PROCEDURES

Article 14. *Inquiries* . Data Subjects or their successors may inquire about the Data Subject's personal information held in any database, whether public or private. The Data Controller or Data Processor must provide them with all the information contained in the individual record or that is linked to the Data Subject's identification.

The inquiry will be made through the means provided by the Data Controller or Data Processor, provided that proof of this can be maintained.

The inquiry will be addressed within a maximum of ten (10) business days from the date of receipt. If it is not possible to address the inquiry within this period, the interested party will be informed, stating the reasons for the delay and indicating the date on which their inquiry will be addressed, which in no case may exceed five (5) business days following the expiration of the first period.

Paragraph. The provisions contained in special laws or regulations issued by the National Government may establish shorter terms, taking into account the nature of the personal data.

Article 15. *Complaints* . The Data Subject or their successors who consider that the information contained in a database should be corrected, updated or deleted, or when they notice the alleged breach of any of the duties contained in this law, may file a complaint with the Data Controller or the

Data Processor, which will be processed under the following rules:

1. The complaint shall be submitted in writing to the Data Controller or the Data Processor, including the Data Subject's identification, a description of the facts giving rise to the complaint, the address, and any supporting documents. If the complaint is incomplete, the interested party shall be notified within five (5) days of receipt of the complaint to remedy the deficiencies. If the applicant fails to provide the required information within two (2) months of the date of notification, the complaint shall be deemed withdrawn.

If the person receiving the complaint is not competent to resolve it, they will forward it to the appropriate person within a maximum of two (2) business days and inform the interested party of the situation.

2. Once the complete claim is received, a note stating "claim in process" and the reason for the claim will be added to the database within no more than two (2) business days. This note must remain until the claim is resolved.

3. The maximum time to address the claim will be fifteen (15) business days, counted from the day following the date of its receipt. If it is not possible to address the claim within this period, the interested party will be informed of the reasons for the delay and the date on which their claim will be addressed, which in no case may exceed eight (8) business days following the expiration of the first period.

Article 16. *Procedural requirement.* The Data Subject or successor may only file a complaint with the Superintendency of Industry and Commerce once the consultation or claim process before the Data Controller or Data Processor has been exhausted.

TITLE VI

DUTIES OF DATA CONTROLLERS AND DATA PROCESSORS

Article 17. *Duties of Data Controllers.* Data Controllers shall comply with the following duties, without prejudice to the other provisions of this law and other laws governing their activity:

- a) Guarantee to the Holder, at all times, the full and effective exercise of the right of habeas data;
- b) Request and keep, under the conditions provided for in this law, a copy of the respective authorization granted by the Holder;
- c) Duly inform the Data Subject about the purpose of the collection and the rights they have by virtue of the authorization granted;
- d) Keep the information under the necessary security conditions to prevent its alteration, loss, consultation, use or unauthorized or fraudulent access;
- e) Ensure that the information provided to the Data Processor is truthful, complete, accurate, up-to-date, verifiable and understandable;
- f) Update the information, promptly informing the Data Controller of any changes to the data previously provided and take other necessary measures to ensure that the information provided to the Data Controller remains up to date;
- g) Rectify the information when it is incorrect and communicate the relevant information to the Data Controller;
- h) To provide the Data Processor, as the case may be, only with data whose processing has been previously authorized in accordance with the provisions of this law;
- i) Require the Processor at all times to respect the security and privacy conditions of the Data Subject's information;
- j) Process inquiries and claims made in accordance with the terms set out in this law;

- k) Adopt an internal manual of policies and procedures to ensure proper compliance with this law and, in particular, to handle inquiries and complaints;
- l) Inform the Data Controller when certain information is under discussion by the Data Subject, once the complaint has been filed and the respective process has not been completed;
- m) Inform the Data Subject, upon request, about the use given to their data;
- n) Inform the data protection authority when security code violations occur and there are risks in the management of the information of the Data Subjects.
- o) Comply with the instructions and requirements issued by the Superintendency of Industry and Commerce.

Article 18. Duties of Data Processors. Data Processors shall comply with the following duties, without prejudice to the other provisions of this law and other laws governing their activity:

- a) Guarantee to the Holder, at all times, the full and effective exercise of the right of habeas data;
- b) Keep the information under the necessary security conditions to prevent its alteration, loss, consultation, use or unauthorized or fraudulent access;
- c) To promptly update, rectify or delete the data in accordance with the terms of this law;
- d) Update the information reported by the Data Controllers within five (5) business days from receipt;
- e) Process the queries and claims made by the Holders in accordance with the terms set out in this law;
- f) Adopt an internal manual of policies and procedures to ensure proper compliance with this law and, in particular, to address inquiries and complaints from Data Subjects;
- g) Register in the database the legend "claim in process" in the manner regulated in this law;
- h) Insert the legend "information under judicial discussion" into the database once notified by the competent authority about legal proceedings related to the quality of the personal data;
- i) Refrain from circulating information that is being disputed by the Holder and whose blocking has been ordered by the Superintendency of Industry and Commerce;
- j) Allow access to the information only to those people who are authorized to access it;
- k) Inform the Superintendency of Industry and Commerce when violations of security codes occur and there are risks in the management of the information of the Holders;
- l) Comply with the instructions and requirements issued by the Superintendency of Industry and Commerce.

Paragraph. In the event that the roles of Data Controller and Data Processor are held by the same person, the person shall be required to fulfill the duties established for each role.

TITLE VII

ON THE MECHANISMS OF MONITORING AND SANCTION

CHAPTER I

From the data protection authority

Article 19. Data Protection Authority . The Superintendency of Industry and Commerce, through a Delegate for the Protection of Personal Data, will exercise oversight to ensure that the principles, rights, guarantees and procedures provided for in this law are respected in the Processing of personal data.

Paragraph 1. The National Government, within six (6) months from the date of entry into force of this law, will incorporate into the structure of the Superintendency of Industry and Commerce an office of Delegate Superintendent to exercise the functions of Data Protection Authority.

Paragraph 2. The monitoring of the processing of personal data regulated in Law [1266](#) of 2008 will be subject to the provisions of said law.

Article 20. *Resources for the exercise of its functions.* The Superintendency of Industry and Commerce shall have the following resources to exercise the functions attributed to it by this law:

a) The resources allocated to it in the General Budget of the Nation.

Article 21. *Functions* . The Superintendency of Industry and Commerce shall perform the following functions:

a) Ensure compliance with legislation on the protection of personal data;

b) To advance the investigations of the case, either ex officio or at the request of a party, and, as a result thereof, to order the measures necessary to enforce the right of habeas data. For this purpose, whenever the right is unknown, it may order that access to and provision of the data, its rectification, updating, or deletion be granted;

c) To order the temporary blocking of data when, from the request and the evidence provided by the Data Subject, a certain risk of violation of their fundamental rights is identified, and such blocking is necessary to protect them while a final decision is adopted;

d) Promote and disseminate the rights of individuals in relation to the processing of personal data and implement educational campaigns to train and inform citizens about the exercise and guarantee of the fundamental right to data protection;

e) To give instructions on the measures and procedures necessary for the adaptation of the operations of the Data Controllers and Data Processors to the provisions provided for in this law;

f) Request from the Data Controllers and Data Processors the information necessary for the effective exercise of their functions.

g) Issue declarations of conformity regarding international data transfers;

h) Administer the National Public Registry of Databases and issue the orders and acts necessary for its administration and operation;

i) Suggest or recommend adjustments, corrective measures or adaptations to the regulations that are in accordance with technological, computer or communicational evolution;

j) To require the collaboration of international or foreign entities when the rights of the Holders are affected outside of Colombian territory on the occasion of, among others, the international collection of personal data;

k) Any other duties assigned to it by law.

CHAPTER II

Procedure and sanctions

Article 22. *Procedure* . The Superintendency of Industry and Commerce, once it has established non-compliance with the provisions of this law by the Data Controller or the Data Processor, will adopt the corresponding measures or impose the corresponding sanctions.

In matters not regulated by this law and the corresponding procedures, the relevant rules of the Administrative Litigation Code shall apply.

Article 23. *Sanctions* . The Superintendency of Industry and Commerce may impose the following sanctions on Data Controllers and Data Processors:

a) Personal and institutional fines up to the equivalent of two thousand (2,000) current legal monthly minimum wages at the time the sanction is imposed. The fines may be successive as long as the non-compliance that originated them persists;

b) Suspension of activities related to the Treatment for up to six (6) months. The suspension order will indicate the corrective measures that must be taken;

c) Temporary closure of operations related to the Treatment once the suspension period has expired without the corrective measures ordered by the Superintendency of Industry and Commerce having been adopted;

d) Immediate and definitive closure of the operation involving the processing of sensitive data;

Paragraph. The sanctions indicated in this article apply only to private individuals. If the Superintendency of Industry and Commerce detects a suspected breach of the provisions of this law by a public authority, it shall refer the matter to the Office of the Attorney General of the Nation for the corresponding investigation.

Article 24. Criteria for determining penalties . The penalties for the infringements referred to in the previous article shall be determined according to the following criteria, insofar as they are applicable:

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

b) The economic benefit obtained by the offender or third parties, by virtue of the commission of the infringement;

c) Recidivism in the commission of the infraction;

d) Resistance, refusal or obstruction to the investigative or surveillance action of the Superintendency of Industry and Commerce;

e) Reluctance or disobedience to comply with orders issued by the Superintendency of Industry and Commerce;

f) The express acknowledgment or acceptance by the investigated party regarding the commission of the infraction before the imposition of the sanction that may be applicable.

CHAPTER III

From the National Database Registry

Article 25. Definition . [Regulated by National Decree 886 of 2014](#), the National Database Registry is the public directory of databases subject to processing that operate in the country.

The registry will be administered by the Superintendency of Industry and Commerce and will be freely accessible to citizens.

To register databases, interested parties must submit their data processing policies to the Superintendency of Industry and Commerce. These policies will be binding on those responsible for and in charge of data processing, and failure to comply will result in the corresponding penalties. The data processing policies may not, under any circumstances, be less stringent than the obligations established in this law.

Paragraph. The National Government will regulate, within one year of the promulgation of this law, the minimum information that the Registry must contain, and the terms and conditions under which the Data Controllers must register therein.

TITLE VIII

DATA TRANSFER TO THIRD COUNTRIES

Article 26. Prohibition . The transfer of personal data of any kind to countries that do not provide adequate levels of data protection is prohibited. A country is considered to offer an adequate level of data protection when it complies with the standards established by the Superintendency of Industry and Commerce on this matter, which in no case may be lower than those required by this law for its recipients.

This prohibition will not apply when it comes to:

- a) Information regarding which the Holder has given his express and unequivocal authorization for the transfer;
- b) Exchange of medical data, when required by the Data Subject's Treatment for reasons of health or public hygiene;
- c) Bank or stock market transfers, in accordance with the legislation applicable to them;
- d) Transfers agreed within the framework of international treaties to which the Republic of Colombia is a party, based on the principle of reciprocity;
- e) Transfers necessary for the execution of a contract between the Data Subject and the Data Controller, or for the execution of pre-contractual measures provided that the Data Subject has given his or her authorization;
- f) Transfers legally required for the safeguarding of the public interest, or for the recognition, exercise or defense of a right in a judicial process.

Paragraph 1. In cases not covered as exceptions in this article, the Superintendency of Industry and Commerce shall issue the declaration of conformity regarding the international transfer of personal data. For this purpose, the Superintendent is authorized to request information and carry out the necessary procedures to establish compliance with the requirements for the viability of the transaction.

Paragraph 2. The provisions contained in this article shall be applicable to all personal data, including those contemplated in Law [1266](#) of 2008.

TITLE IX

OTHER PROVISIONS

Article 27. Binding Corporate Rules . The National Government will issue the corresponding regulations on Binding Corporate Rules for the certification of good practices in the protection of personal data and its transfer to third countries.

Article 28. Transitional Regime . Persons who, on the date of entry into force of this law, carry out any of the activities regulated herein shall have a period of up to six (6) months to adapt to the provisions contemplated in this law.

Article 29. Repeals . This law repeals all provisions that are contrary to it, with the exception of those contemplated in Article 2.

Article 30. Validity . This law shall enter into force upon its promulgation.

The President of the Honorable Senate of the Republic,

ROY LEONARDO BARRERAS MONTEALEGRE.

The Secretary General of the Honorable Senate of the Republic,

GREGORIO ELJACH PACHECO.

The Speaker of the Honorable House of Representatives,

AUGUSTO POSADA SÁNCHEZ.

The Acting Secretary General of the Honorable House of Representatives,

FLOR MARINA DAZA RAMÍREZ.

REPUBLIC OF COLOMBIA – NATIONAL GOVERNMENT

PUBLISH AND COMPLY.

In compliance with the provisions of Judgment C-748 of 2011 issued by the Constitutional Court, the bill is sanctioned, which orders the referral of the file to the Congress of the Republic, to continue the rigorous procedure and subsequent sending to the President of the Republic.

Given in Bogotá, DC, on the 17th day of October 2012.

JUAN MANUEL SANTOS CALDERÓN

The Minister of Justice and Law,

RUTH STELLA CORREA PALACIO.

The Minister of Finance and Public Credit,

MAURICIO CÁRDENAS SANTA MARÍA.

The Minister of Trade, Industry and Tourism,

SERGIO DIAZ-GRANADOS GUIDA.

The Minister of Information and Communications Technologies,

DIEGO MOLANO VEGA.

NOTE: Published in the Official Gazette 48587 of October 18, 2012.

Go back



Gobierno de Colombia



- Vice Presidency
- Ministry of Justice
- Ministry of Defense
- Ministry of Labor
- Ministry of the Interior
- MinCiencias
- Ministry of Foreign Affairs
- Ministry of Finance
- Ministry of Health
- Ministry of Energy
- Ministry of Commerce
- Ministry of Sport
- MinTIC
- Ministry of Education
- Ministry of Culture
- Ministry of Agriculture
- Ministry of Environment
- Ministry of Transport
- Ministry of Housing
- Glass Urn



PUBLIC SERVICE



Carrera 6 # 12-62,
Bogotá DC



Postal Code: 111711
Telephone Switchboard: (+57) 601 5956600
National Toll-Free Line: 018000931186



www.funcionpublica.gov.co
Contact Email: eva@funcionpublica.gov.co
Legal notifications:
notificacionesjudiciales@funcionpublica.gov.co

CONTACT

In-person service hours for the Citizen Service group:
Monday to Friday, 7:30 am to 6:00 pm

Mail reception:
Monday to Friday, 8:00 am to 4:00 pm Continuous schedule

CITIZEN SERVICES

- Court notifications
- Notification of administrative acts
- Notifications to third parties
- Allegations of corruption
- Citizen participation
- Frequently Asked Questions
- Submit your PQRS request
- Site map
- Login to institutional email
- Site statistics
- Access