Friday, 17th June, 2011 III Series – Nº 114

STATE GAZETTE

OFFICIAL ORGAN OF THE REPUBLIC OF ANGOLA

Price - KZ: 220,00

All correspondence either official related to announcements and subscription of the State Gazette, should be directed to National Printing House - U.E.E.inLuanda, CP 1306 –EndTeleg.; «Imprensa».	SUBSCRIPTIONS The three series. ... KZ 440,375.00 The 1st series ... KZ 260.250.00 The 2nd series... KZ 135.850.00 The 3rd series ... KZ 105.700.00	The price of each line published in the State Gazette 1st and 2nd series is KZ 75.00. and for the 3rd series is KZ 95.00, plus therespective stamp duty, depending on the publication of the 3rd series of the previous deposit to conduct in the National Printing House - U.E.E ..

SUMMARY

NATIONAL ASSEMBLY
Law Nr. 22/11
of 17th June

The protection of personal data, confidentiality and the reserve of private life is of fundamental importance in the context of safeguarding the fundamental rights of citizens, recognized by the Universal Declaration of Human and Peoples' Rights.

The consecration, in the Constitution of the Republic of Angola, of the right to reserve private life and the possibility of recourse to "habeas data" representation is clearly a major step in the adoption of a legislative framework in this matter.

The right to privacy is also reflected in the respect for the privacy of citizens in relation to the processing of personal data concerning them. Even though such treatment has a relevant role in improving the well-being of citizens and economic progress in a context of boosting and developing a greater variety of services, particularly in the scope of technologies and the information society, it is necessary to ensure that it be done in a context of respect for your privacy.

The National Assembly approves, by mandate of the people, under the terms of paragraph 2 of article 165 and paragraph d) of paragraph 2 of article 166, both of the Constitution of the Republic of Angola, the following:

PERSONAL DATA PROTECTION LAW

CHAPTER I
General Provisions

ARTICLE 1
(Object)

The purpose of this law is to establish the Legal Rules Applicable to the processing of personal data with the aim of guaranteeing respect for public freedoms and the fundamental rights and guarantees of natural persons.

ARTICLE 2
(Objective scope)

This law applies to the processing of personal data carried out by fully or partially automated means of personal data contained in or intended for manual purposes.

ARTICLE 3
(Scope of Subjective and Territorial Application)

1. The processing of personal data by any person and entity in the public, private or cooperative sector is subject to this law.

2. This law applies to the processing of personal data carried out:

   a) responsible for the treatment based in the Republic of Angola;
   b) within the scope of the activities of the controller responsible for the treatment established in the Republic of Angola, even though the said controller does not have its headquarters in Angolan territory;
   c) outside the Republic of Angola, where the Angolan legislation is applicable under private international public law;
   d) by a controller, who, not being established in the Republic of Angola, uses means located in Angola to process personal data.

3. For the purposes of subparagraph d) of the previous number, the controller is considered to use means located in Angolan territory when the processing of personal data is carried out with, or personal data is housed in, means located in Angolan territories, for the purposes of this law, the mere use of such means for the collection, registration or transit of personal data in the territory of the Republic of Angola is sufficient.

4. In the case of paragraph d) of paragraph 2 of this article, the controller must designate, by means of a communication to the Data Protection Agency, a representative established in the Republic of Angola to replace him in all rights and obligations, without prejudice to their own responsibility.

ARTICLE 4
(Exclusions)

1. This law does not apply to the processing of personal data, carried out by a natural person in the exercise of exclusively personal or domestic activities.

2. Without prejudice to the provisions of special legislation, the processing of personal data in the following circumstances is also excluded from the present law:

   a) The processing of personal data under the rules, legal applicable to State secrecy and security, as well as the secrecy of justice;

b) The processing of personal data of members of the Angolan Armed Forces by the units, military or other establishments and bodies under the responsibility of the ministerial department responsible for the Armed Forces.

ARTICLE 5
(Definitions)

For the purposes of this law, the following definitions apply:

a) consent of the data subject: any expression of free will, specific, explicit and informed, regardless of the medium, in which the data subject authorizes its processing;
b) personal data: any information, whatever its nature or support, including image and sound, relating to an identified or identifiable natural person (data subject). An identifiable person is one who can be identified, directly or indirectly, namely by reference to an identification number or the combination of specific elements of his physical, physiological, psychological, economic, cultural or social identity;
c) sensitive data: personal data relating to philosophical or political beliefs, party or union affiliation, religious faith, private life, racial or ethnic origin, health and sexual life, including genetic data;
d) recipient: the natural or legal person, the public authority or any other body to whom personal data are communicated, regardless of whether it is a third party or not;
e) personal data file (file): any structured set of personal data, regardless of the form or modality of creation, organization, conservation and access to the data, whether centralized, decentralized or distributed in a functional or geographic way;
f) publicly accessible sources: files that are intended for information to the public and are open to public consultation or to a third party with a legitimate interest, and whose consultation is not subject to restrictions, except for the payment of an accessible monetary value. Publicly accessible sources are considered, without prejudice to other files that meet the indicated requirements, official diaries and bulletins, the media, telephone guides under the terms of the applicable legislation and lists of people belonging to a particular professional group and that contain only your name, title, profession, activities, academic degree and address;
g) data interconnection: form of treatment of personal data that consists of the possibility of relationships between the data in a file with the other responsible or the same responsible for other purposes;
h) advertising messages: any form of communication made by persons or entities in the public or private sector, within the scope of a commercial, industrial, artisanal or liberal activity, with the direct or indirect objective of promoting ideas, principles, initiatives or institutions;
i) controller: the natural or legal person, the public authority or any other body that, individually or jointly with others, determines the purposes and means of processing personal data. Whenever the purposes and means of treatment are determined by legislative, regulatory or other provisions, the controller must be indicated in the respective diploma;
j) cooperative sector: cooperatives and entities of a mutual nature, as well as others indicated, in specific legislation;
k) private sector: private natural and legal persons;
l) public sector: the State, public administration bodies, criminal prevention, investigation and repression bodies and the courts;
m) subcontractor: the natural or legal person, the public authority or any other body that processes personal data on behalf of the controller under a contractual relationship established with him;

n) third party: the natural or legal person, the public authority or any other bodies that, not being the data owner, the controller, the subcontractor or another person under the direct authority of the controller or the subcontractor or another person under authority directly responsible for the controller or the subcontractor, has access and is qualified to process the data;
o) processing of personal data (processing): any operation or set of operations carried out on personal data, with or without autonomous means, such as the collection, registration, organization, conservation, adaptation or alteration, recovery, consultation, use, communication by transmission, broadcast or any other form of provision, with comparison or interconnection, as well as blocking or destruction.

CHAPTER II
Treatment of Personal Data

SECTION I

ARTICLE 6
(Principles of transparency)

1. The processing of personal data must be carried out in a transparent manner, in writing respecting the principle of private reserve, as well as the fundamental public rights, freedoms and guarantees provided for in the Constitution of the Republic of Angola and in this law.

2. For the purposes of the preceding paragraph, personal data must in particular be kept in a manner that allows the holders of the rights of access, information, rectification, cancellation and opposition, as provided for in this law.

ARTICLE 7
(Principles of lawfulness)

1. The processing of personal data must be carried out in a lawful and loyal manner, with respect for the principle of good faith.

2. The processing of personal data that leads to arbitrary and lawful discrimination in relation to its holder is considered contrary to the principle of good faith.

ARTICLE 8
(Principles of proportionality)

Personal data subject to processing must be relevant, adequate and not excessive in relation to the purposes that legitimized its collection and processing.

ARTICLE 9
(Principles of purpose)

1. Personal data must be collected and processed for purposes: determined, explicit and legitimate as defined in a specific diploma.

2. The processing of personal data for purposes other than or incompatible with those that originated its collection and processing is prohibited, unless:

   a) the data processing has given its express consent;
   b) the processing has historical or statistical purposes and the data are anonymized for this purpose;
   c) the treatment has as its objective the prevention, investigation and criminal repression, or national security of the terms admitted by specific legislation, as long as the rights, freedoms and guarantees of the data subjects should not prevail.

ARTICLE 10
(Principle of veracity)

1. Personal data subject to processing must be accurate.

2. Appropriate measures must be taken to ensure that the total or partially inaccurate or incomplete are erased or rectified, so that they correspond to the current and concrete situation of the holder.

ARTICLE 11
(Principles of the duration of the conservation period)

1. Personal data must be kept in such a way as to permit the identification of its holders only for the period necessary to pursue the purposes that led to its collection or treatment, and must be subsequently deleted or taken anonymously.

2. The preservation of personal data for historical, statistical, criminal investigation and national security purposes may be authorized by the Data Protection Agency for a longer period upon request of the person responsible for the treatments.

SECTION II
Requirements for the Processing of Personal Data

ARTICLE 12
(General requirements for the processing of personal data)

1. Subject to a legal provision to the contrary, the processing of personal data can only be carried out under the following circumstances:

   a) unequivocal and express consent of its titleholder;
   b) notification to the Data Protection Agency.

2. Without prejudice to the provisions of article 25, the consent of the data subject is not necessary when processing is necessary to:

   a) execution of contracts or contracts to which the data subject is a party or due diligence prior to the formation of the contract or negotiation declaration made at his request:

b) compliance with a legal obligation that the controller is subject to:
c) protection of vital interests of the data subject, by his legal representative if he is physically or legally unable to give his consent;
d) carrying out a mission of public interest or exercising public authority in which the controller or a third party to whom the data is communicated is invested;
e) pursuit of legitimate interests of the controller or of a third party to whom the data is communicated, provided that the interests or rights, freedoms and guarantees of the data subject should not prevail.

ARTICLE 13
(Specific requirements for the processing of sensitive data)

1. Unless otherwise specified, the processing of personal data can only be carried out if the following circumstances are met:

   a) legal provision that allows such treatment;
   b) authorization from the Data Protection Agency, which can only be granted, subject to at least one of the following conditions:
   i) the processing of data to be carried out with the unequivocal, express and written consent of its owner or his legal representative;
   ii) the processing of the data is carried out with the unequivocal and express consent of the holder by foundation, association or non-profit organizations of a political, philosophical, religious or union nature, within the scope of their, legitimate activities, on condition that the processing only respects members of that body or persons who maintain regular contact with them for their purposes, and that the data are not communicated to third parties without the clear and express consent of their holders;
   iii) the need to protect vital interests of the data subject or another person and the data subject is physically or legally unable to give consent;
   iv) the data in question are manifestly made public by their owner, provided that they can legitimately deduce consent from their declarations for the treatment of them;
   v) the processing of data is necessary for the declaration, exercise or defense of a right in judicial process and is carried out exclusively for that purpose;
   vi) the processing of the data is, for reasons of public interest, indispensable for the exercise of legal or statutory powers of the person in charge, including for the exercise of the investigative activities of the judicial, police and administrative authorities within the scope of their powers.

2. The processing of sensitive data resulting from a legal provision must be modified by the Data Protection Agency.

3. The processing of sensitive data must be carried out with guarantees of non-discrimination and through the adoption of special security measures.

ARTICLE 14
(Specific requirements for the processing of sensitive health and sexual life data)

1. Without prejudice to the provisions of the previous article and to special legislation, the processing of personal data relating to health and sexual life, including genetic data, which are considered sensitive data, can only be carried out if the following circumstances are verified:

a) unequivocal, express and written consent of its owner or his legal representative: and / or
b) authorization from the Data Protection Agency

2. The processing of the data indicated in the previous number is allowed without the consent of the data subject, when it is necessary for the purpose of preventive medicine, medical diagnosis, medical assistance, management and statistics of health services or in the case of medical emergency or justified in the public interest.

3. The processing of health and sexual life data must be carried out by a health professional registered in the corresponding professional order, obliged to comply with the duty of professional secrecy.

ARTICLE 15
(Specific requirements for the processing of data reactive to illegal activities, crime and misdemeanors)

1. The processing of personal data relating to persons subject to illegal activities, criminal offenses, misdemeanors and penalties, security measures, fines and accessory sanctions, which are considered sensitive data, can only be carried out by public authorities, verified following circumstances:

   a) legal provision that allows such treatment by authorities with specific powers, in compliance with the procedural and data protection rules provided for by law and with the prior opinion of the Data Protection Agency; or
   b) authorization from the Data Protection Agency, which can only be granted when such treatment is necessary for the execution of legitimate purposes of its responsible and the data protection and information security rules are observed.

2. Without prejudice to the provisions of specific legislation, the processing of personal data for the purposes of police investigation must be limited to what is necessary for the purposes of general and special prevention or the suppression of a specific offense, under the terms of this law and of special legislation.

ARTICLE 16
(Specific requirements for the processing of credit and solvency data)

1. Without prejudice to the provisions of paragraph 2 of this article, the processing of personal data relating to credit and solvency can only be carried out if the following circumstances are verified, unless the information is obtained from publicly accessible sources in compliance with its conditions of consultation and use:

   a) unequivocal, express and written consent of the data subject;
   b) authorization from the Data Protection Agency.

2. The processing of credit and solvency data related to the fulfillment and non-fulfillment of credit obligations by the person responsible is subject to:

   a) notification to the holder that his / her data are included in the debtor's file of the person responsible, and such notification must be made within sixty days after insertion of the data in such files;
   b) authorization from the Data Protection Agency.

ARTICLE 17
(Specific requirements for the processing of data in video surveillance systems and other means of electronic control)

1. The processing of personal data in the scope of the installation of video surveillance systems and other forms of capturing, processing and disseminating sounds and images that allow the identification of people including electronic road surveillance systems, is subject to the provisions of article 13.

2. The controller must make available, in places with video surveillance systems, information regarding their existence, the capture of sound and images and the name of the person responsible for processing the data, his address, telephone number and e-mail.

3. The rules applicable to the installation of video surveillance systems and the treatment of data collected in this context will be set out in special legislation.

ARTICLE 18
(Specific requirements for the processing of data for the purpose of advertising by post)

1. The processing of personal data for the purpose of sending advertising messages addressed to the home, by post or by direct distribution, is permitted by notification to the Data Protection Agency, except when the recipient has expressly opposed the treatment and use your data for this purpose.

2. For the purposes of the provisions of the previous number, the holder must have access to means that allow him at any time to refuse, free of charge, free of charge and regardless of just cause, the sending of such advertising for the future.

3. In the event of opposition, entities that promote the sending of advertising messages to the home by post or by direct distribution must maintain a list of holders who have expressed their opposition to the sending of such messages.

4. The processing of personal data for the purposes provided for in paragraph 2 above does not require notification to the Data Protection Agency, nor the consent of the data subjects.

5. With a view to making the provisions of paragraph 2 of this article more effective, the Data Protection Agency shall support the establishment of lists of holders who have expressed their opposition sending advertising messages.

6. The person responsible for processing personal data for the purposes of this article must inform the recipient:

   a) on the origin of your personal data, if they originate from sources accessible to the public;
   b) that your data will be communicated to recipients for advertising purposes, if the data subject has consented, in which case the requirements for data communication contained in article 21 are observed;
   c) on the identity of the controller, the sending of advertising by post or direct distribution being forbidden, concealing or concealing the identity of the person in the name of who is communicating.

ARTICLE 19
(Specific requirements for processing data for electronic advertising purposes)

1. The processing of personal data for the purpose of sending advertising messages addressed by electronic means, namely by means of automatic calling devices, fax machines or electronic mail, is subject to the following requirements:

   a) unequivocal and express consent of the recipient of such messages;
   b) notification to the Data Protection Agency.

2. The processing of personal data for the purposes provided for in the preceding paragraph may be carried out without the consent of the data subject in the following circumstances:

   a) when messages are sent to the data subject as a representative, worker or collaborator of a legal person;
   b) when messages are sent by the Public Administration through the electronic governance systems of the Angolan Executive;
   c) when the messages are sent to natural persons with whom the supplier of the product or the service provider has previously entered into transactions, if it has been explicitly possible to refuse during the transaction carried out and if it does not involve additional expenditure to the recipient cost of telecommunications service.

3. In the case provided for in the preceding paragraph, the data subject has the right to object to its processing for the purposes set out in this article.

4. For the purposes of the provision in the previous number, the holder must have access to means that allow him at any time to refuse, free of charge, free of charge and regardless of just cause, the sending of such advertising for the future.

5. In case of opposition, the entities that promote the sending of advertising messages must maintain an updated list, by themselves or by organizations that represent them, of holders who have expressed their opposition to the sending of such messages.

6. The processing of personal data for the purposes provided for in paragraph 2 above does not require notification to the Data Protection Agency, nor the consent of the data subjects.

7. With a view to making the provisions of paragraph 2 of this article more effective, the Data Protection Agency supports the establishment of lists of holders who have expressed their opposition to the sending of advertising messages.

8. The person responsible for processing personal data for the purposes of this article must inform the recipient:

   a) on the origin of your personal data, if they originate from sources accessible to the public;
   b) that your data will be communicated to recipients for advertising purposes, if the data subject has consented, in which case the requirements for data communication contained in article 21 are observed;

c) on the identity of the controller, the sending of advertising by post or direct distribution being forbidden, concealing or concealing the identity of the person in the name of who is communicating.

ARTICLE 20
(Specific requirements for recording calls)

1. The recording of calls is admitted when carried out within the scope of legal commercial practices, for the purpose of proving a commercial transaction, provided that:

   a) the data subject has previously given his express and unequivocal consent to the recording, which must start with the registration of the consent;
   b) the Data Protection Agency has authorized such processing.

2. Except for the need for the data subject's consent and prior authorization from the Data Protection Agency, recordings of communications to and from public services designed to provide emergency situations of any kind.

3. In the case foreseen in the previous number, data processing is subject to prior notification to the Data Protection Agency.

SECTION III
Communication and Interconnection of Personal data

ARTICLE 21
(Data communication)

The communication of personal data by the person responsible to a recipient is subject to the following rules:

a) if personal data are communicated to the recipient for the purpose of pursuing his / her own purposes, the recipient will also be considered responsible for the processing of the same, and must comply with the legal provisions that apply to him / her;
b) if the personal data are communicated to the recipient for the purposes of pursuing the purposes of the responsible person who communicates the data, treating the recipient the data in the name and on behalf of the responsible person, the recipient is considered a subcontractor, and must comply with the legal provisions that apply to it;
c) if the personal data are communicated to the recipient, none of the conditions mentioned in the previous points are met, and the latter is not under the direct authority of the controller or processor, the recipient will be considered a third party.

ARTICLE 22
(Communication of data to person responsible for processing or to a third party)

1. The communication of data to a recipient who is also responsible for the processing or who is a third party can only be carried out if verified circumstances:

a) unequivocal and express consent of the recipient of such messages;
b) notification to the Data Protection Agency.

2. The communication of data is not subject to the prior consent of the holder when:

a) the communication follows from a law or a judicial decision;
b) the data have been collected from publicly accessible sources in compliance with their conditions of consultation and use, applicable to such sources;
c) the communication of data is necessary for the execution of contracts or contracts to which the data subject is a party or due to previous steps in the formation of the contract or negotiation declaration made at his request:
d) the communication of data is necessary for the fulfillment of a legal obligation to which the controller who transmits the data or the recipient are subject, as happens if the communication is for the purpose of carrying out the activities assigned to the Courts (including the Court of Accounts), the Public Ministry, the Ombudsman and the defense and security bodies of the Angolan Study;
e) the conditions that legitimate the processing of personal data are verified without the consent of the holder under the terms of articles 12 to 20 of this law.

3. The communication of credit and solvency data between banking institutions and those authorized by law and of investigation and criminal introduction can be done without the prior consent of the data subject, with prior authorization from the Data Protection Agency.

ARTICLE 23
(Communication of data to subcontractors)

1. The communication of data to a subcontractor can only be carried out under the following circumstances:

a) conclusion of a contract or other document with legal value, reduced to writing whose content establishes the obligation of the subcontractor to comply with the provisions of this law and to act in accordance with the instructions of the controller;
b) notification to the Data Protection Agency.

2. Unless the controller instructs the subcontractor to the contrary, it is subject to the following obligations:

a) obligation not to communicate personal data to other recipients:
b) obligation to comply with the safety measures established in the present law;
c) obligation to destroy personal data or to return them to the controller after the contractual relationship ends.

3. The subcontractor cannot process personal data for its own purposes, nor can it communicate it to other recipients in disregard of the previous number, under the risk of, if it does, being considered responsible for the processing of the same.

4. The provisions of this article are applicable to any personal data processing operation carried out by a subcontractor.

ARTICLE 24
(Interconnection of personal data)

1. The interconnection of personal data may only be carried out with the authorization of the Data Protection Agency, unless it is provided for by law.

2. The Data Protection Agency only authorizes data interconnection if the interconnection;

   a) it is appropriate to pursue the legal or statutory purposes and the legitimate interests of the controllers;
   b) does not imply discrimination, injury or reduction of the rights, freedom and fundamental guarantees of the data subjects; and
   c) is surrounded by adequate measures and security levels.

Section IV
Rights of data subjects

ARTICLE 25
(Interconnection of personal data)

1. Without prejudice to the provisions of other articles of this law, the controller must make available to data subjects at least the following information:

   a) the identity and address of the controller;
   b) the purposes of the processing and the creation of a file for that purpose;
   c) the recipients or categories of recipients of the data;
   d) the mandatory or optional nature of the response, as well as the possible consequences of not responding;
   e) the existence and conditions of the right of access and of reification, updating, elimination and opposition;
   f) consequences of data collection without the consent of the owner or, in the event of his incapacity, by his legal representative;
   g) other information necessary to guarantee the lawful treatment of such personal data.

2. When personal data are collected directly from the data subject, the information must be provided at the time of collection, unless it has already been provided at a previous time.

3. If personal data are not collected directly from the data subject responsible for processing, they must provide the information referred to at the time of registration of the data or at the latest within 30 days after its collection, unless it is already known about it .

4. Information must be provided in a clear, precise and objective manner, in particular when it is addressed to minors and people with special needs.

5. The obligation to provide information may be waived by means of a legal provision or a decision by the Data Protection Agency, in the following cases:

   a) for reasons of State security and criminal prevention or investigation;

b) when the provision of information to the data subject proves to be impossible or implies disproportionate efforts, particularly in cases of data processing for statistical, historical or scientific research purposes; or
c) when the law expressly determines the registration of data or its disclosure.

6. The information obligation, under the terms of the previous number, does not apply to the processing of data carried out for exclusively journalistic purposes or that of artistic or illiterate expression.

7. In the case of data collection in open networks, the right to information is considered provided through the publication of publication and availability of privacy policies that are easily accessible and include:

a) the information described in paragraph 1 of this article;
b) the information that your personal data can circulate on the network without security conditions, at the risk of being seen and used by unauthorized third parties.

ARTICLE 26
(Right of access)

1. The data subject has the right to obtain from the controller freely, without restrictions, delays or excessive costs, information about what is incurred and the recipients or categories to whom the data is communicated.

2. The controller must also communicate to the data subject the specific data being processed, as well as any information about the origin of such data.

3. Without prejudice to the provisions of specific legislation, in the treatment of personal data reactive to State security, prevention or criminal investigation and to the secrecy of justice, the right of access is exercised through the Data Protection Agency.

4. When processing personal data for purely journalistic purposes, the right of access is exercised by the Data Protection Agency, safeguarding the applicable constitutional rules, namely those that guarantee Data Protection.

5. In the case provided for in paragraphs 3 and 4, if access to the data by the data subject may impair the security of the State, the prevention or criminal investigation, secrecy of justice or even freedom of expression and freedom of the press, the Agency for Data Protection is limited to informing the data owner of the diligence carried out.

6. The law restrict the right of access verified the following circumstances:

a) the data are not used to take measures or decisions in relation to specific persons, but exclusively for the purpose of scientific research or kept in the form of personal data for a period not exceeding what is necessary for the sole purpose of compiling statistics;
b) there is no danger of violation of the fundamental rights, freedoms and guarantees of the holder of personal data, namely the right to privacy.

7. The data subject's right of access to information on health and sexual life data, including genetic data, is exercised through a physician chosen by the data subject or his legitimate representative.

ARTICLE 27
(Right of opposition)

The data subject is entitled to:

a) unless legally provided to the contrary, and at least in the situations referred to in paragraphs d) and e) of paragraph 2 of article 12, oppose at any time that the data concerning it be processed when there are ponderous and legitimate reasons related to their particular situation, in which case the responsible person should exclude such data from treatment;
b) oppose the processing of your data in other circumstances provided for in this law and other specific legislation.

ARTICLE 28
(Right to rectify, update and delete)

1. The holder of personal data is guaranteed the rights to rectify, update or delete his personal data whose treatment does not comply with the provisions of the present law, namely due to the incomplete or inaccurate nature of those working days.

2. The controller is obliged, under the terms of the present law and special legislation, to ensure the right to update and delete data in a period of sixty working days.

3. If the data subject to update or elimination rectification has been previously communicated to the recipient, the controller is obliged to notify the said rectification update or elimination, unless this is proven impossible and the recipient must act accordingly.

4. In the case provided for in the preceding paragraph, the recipient who processes the data for his own purposes or for the purposes of a third party may not proceed with the deletion of the data, in which case the recipient must inform the data holder of this situation and confirm whether he wishes also rectify update or delete your data from the respective files.

5. The controller must however block and / or retain personal data in the following cases:

a) legal provision or order of competent authority that compels the controller to block and / or keep the data for a certain period of time;
b) if the blocking and / or preservation of data is necessary to pursue a legitimate interest of the controller, namely for the exercise of a right or for the fulfillment of legal obligations;
c) if the data are being used for the purpose of criminal investigation;
d) if the data deal with data reactive to credits and solvency, while the holder's credit status is not regularized.

ARTICLE 29
(Automated individual rights)

1. Anyone has the right not to be subject to a decision that has an effect on its legal sphere or that significantly affects it, taken exclusively on the basis of an automated processing of data designed to assess certain aspects of its personality, namely its professional capacity your credit the self confidence is worthy or your behavior.

2. Without prejudice to compliance with the remaining provisions of this law, a person may be subject to a decision taken under the terms of the preceding paragraph, provided that this occurs within the scope of the conclusion or execution of a contract and on condition that his request for conclusion or execution of the contract has been satisfied, or that adequate measures exist to guarantee the defense of its legitimate interests, namely its right of representation and expression.

3. A decision may also be allowed under the terms of paragraph 1 of this article when the Data Protection Agency authorizes it, with measures to guarantee the defense of the legitimate interests of the data subject.

SECTION V
Security measures

ARTICLE 30
(Security of processing)

1. The person responsible for the processing must implement the technical and organizational measures, and establish adequate security levels, to protect personal data against total or partial, accidental or legal destruction, accidental loss, total or partial alteration, diffusion or unauthorized access, fundamentally when the treatment involves its transmission in network, and against any other form of illegal treatment.

2. Security measures, taking into account the available technical knowledge and the costs resulting from its application, an adequate level of security in relation to the risks that the treatment presents and the nature of the data to be protected.

3. The person responsible for the processing must prepare a document with the security measures, rules and procedures applicable to the processing of personal data, detailing the security levels, the resources to be protected and the functions and obligations of the persons with access to the data, in accordance with safety rules.

ARTICLE 31
(Special security measures)

1. The person responsible for the processing must for the data indicated in Articles 13 to 17 and in Article 20, take appropriate measures to:

   a) prevent unauthorized persons from accessing the files and installations used to process such data;
   b) prevent personal data carriers from being read, copied, altered or removed by an unauthorized person;
   c) prevent unauthorized introduction, as well as acknowledgment of unauthorized alteration or deletion of inserted personal data;

d) prevent automated data processing systems from being used by unauthorized persons through data transmission facilities;
e) ensure that only authorized persons can access the data covered by the authorization;
f) ensure the verification of the entities to whom personal data may be transmitted through the data transmission facilities;
g) ensure that it is possible to verify a posteriori, within an appropriate period, the nature of the treatment as set out in regulations applicable to each sector, which personal data are introduced, when and by whom;
h) to prevent, in the transmission of personal data, as well as in the transport of its support, the data can be read, copied, altered or deleted in an unauthorized manner.

2. The systems must guarantee the logical separation between the data referring to. health and sexual life, including genetic, of other personal data.

3. The Data Protection Agency may determine that, in cases where the network circulation of personal data referred to in articles 12 and 13 to 17, the transmission, encryption, may jeopardize the rights, freedoms and guarantees of the respective holders.

ARTICLE 32
(Professional secrecy)

1. Those responsible for the processing of personal data, as well as persons who, in the exercise of their functions, are aware of the personal data processed are bound by professional secrecy even after the end of their duties.

2. The provisions of the preceding paragraph apply to members of the Data Protection Agency, as well as to employees, agents or technicians who exercise advisory functions to the Data Protection Agency, after the end of the mandate.

3. The provisions of the preceding paragraphs do not exclude the obligation to provide mandatory information, under legal terms, except when they are included in files organized for statistical purposes.

4. Violation of professional secrecy requires its authors criminal liability, under the terms of article 58 of this law, without prejudice to disciplinary or civil liability, under the terms of the law.

SECTION VI
International Transfer of Personal Data

ARTICLE 33
(Data transfer to countries that provide an adequate level of protection)

1. The international transfer of data to countries that ensure an adequate level of protection is subject to notification to the Data Protection Agency.

2. It is understood that a country ensures an adequate level of protection when it guarantees, at least, a level of protection equal to that established in the present law.

3. It is up to the Data Protection Agency to decide whether a State ensures an adequate level of protection, by issuing an opinion in this regard.

4. The adequacy of the level of data protection in a State is assessed by the Data Protection Agency according to all the circumstances surrounding the transfer or set of data transfers, taking into account in particular the nature of the data, the purpose and the duration of the planned treatment or treatments, to the countries of final destination and the rules of law, general or sector, in force in the State concerned, including the professional rules and security measures that are respected in that Study.

ARTICLE 34
(Data transfer to countries that do not provide an adequate level of protection)

1. The international transfer of data to countries that do not provide an adequate level of protection is subject to notification to the Data Protection Agency, which can only be granted if one of the following circumstances or other constants of specific legislation is verified:

   a) if the data subject has given his unambiguous, express and written consent;
   b) if the international transfer of data results from the application of international treaties or agreements to which the Republic of Angola is a party;
   c) if the data transfer is for the sole purpose of responding to or requesting humanitarian aid;
   d) if the transfer of data is necessary for the performance of a contract between the data subject and the person responsible for processing or prior steps 3 formation of the contract decided at the request of the data subject;
   e) if the transfer of data is necessary for the performance or conclusion of a contract in the interest of the data subject between the controller and a third party;
   f) if the transfer of data is necessary or legally required for the protection of an important public interest or for the declaration the exercise or defense of a right in a judicial process;
   g) if the transfer of data is necessary to protect the vital interests of the data subject, or for prevention, diagnosis or medical treatment and the data subject is physically or legally unable to give consent;
   h) if the data transfer is carried out from a publicly accessible source;
   i) if the recipient of the data ensures contractually, before the controller an adequate level of protection for the transferred data.

2. It is the responsibility of the Data Protection Agency to determine the specific conditions that must be included in the contract referred to in paragraph i) of the previous number.

3. In the case of international data transfer between companies of the same business group, the guarantee of compliance with an adequate level of protection can be achieved through the adoption of uniform internal rules on privacy and data protection whose compliance is mandatory.

Section VII
Formality for Notification and Obtaining Authorization from the Data Protection Agency

ARTICLE 35
(Obligation to notify or obtain authorization)

1. Without prejudice to the provisions of this law, the processing of personal data is subject to prior notification to that of the Data Protection Agency or its authorization.

2. If mere notification is necessary, the Data Protection Agency must give its opinion on the request of the controller within thirty days, after receiving it, after which it is understood that the treatment was duly notified.

3. The Data Protection Agency may authorize the simplification or exemption from notification for certain categories of processing which, taking into account the specificity of the data, are not likely to call into question the fundamental rights, guarantees and freedoms of the data subjects, and taking into account taking into account criteria of celebrity, economy and efficiency.

4. The exemption authorization must, among other aspects, specify the purposes of processing the data or categories of data to be processed, the category or categories of data, the recipients or categories of recipients to whom the data may be communicated and the retention period. of the data.

5. Treatments whose sole purpose is to maintain records that are intended for the information of the public and that can be consulted by the general public or by any person with a legitimate interest are exempt from notification.

6. It is not necessary to obtain authorization from the Data Protection Agency if the treatment results from a legal diploma, in which case it is sufficient to proceed with mere notification, unless otherwise indicated in specific legislation.

ARTICLE 36
(Content of notifications and requests for authorization)

Notifications and requests for authorization sent to the Data Protection Agency must contain the following information:

a) name and address of the controller e. if applicable. your representative;
b) purposes of treatment:
c) description of the category or categories of data subjects and of the data or categories of personal data that respect them;
d) recipient or categories of recipients to whom the data may be communicated and under what conditions;
e) entity in charge of processing the information, if it is not the data controller himself.
f) any interconnections of processing personal data;
g) retention time of personal data;
h) forms of conditions in which data subjects can exercise their rights;
i) transfer of planned data to third countries;
j) general description that allows a preliminary assessment of the adequacy of the measures taken to guarantee the safety of the treatment.

ARTICLE 37
(Mandatory information)

The records of personal data processing and the authorization of the Data Protection Agency must at least indicate:

a) the person responsible and, if applicable, his representative;
b) the categories of personal data processed;
c) the purposes for which the data are intended and the categories of entities to whom they may be transmitted;
d) the form of exercising the right of access for rectification. Update and cancellation;
e) any interconnections in the processing of personal data;
f) planned data transfers to third countries;

2. Any alteration of the indications contained in the previous number is subject to the procedures provided for in article 35.

ARTICLE 38
(Advertising of processing)

1. The processing of personal data, when it must be authorized or notified, it is registered with the Data Protection Agency, open to public consultation.

2. The register contains the information listed in points a) to d) and i) of article 36.

3. The controller who is not subject to notification is obliged to provide. Properly. Anyone who requests it, at least the information indicated in paragraph 1 of article 37.

4. The provisions of this article do not apply to the processing of data in publicly accessible lenses.

Section VIII
Specific Provisions Applicable to the Processing of Personal Data in the Public Sector

ARTICLE 39
(Applicable rules)

The processing of data by the public and cooperative sector is subject to:

a) the provisions of this law;
b) the provisions of the specific rules contained in this section and special legislation.

ARTICLE 40
(Creation, modification and deletion)

1. The creation, modification and deletion of files of the Public Administration and Courts can only be carried out under a legal provision, which must contain, expressly or by reference to an autonomous diploma, the following information:

   a) the person responsible for the workers;
   b) the purposes of the treatment;
   c) those for the collection and processing of personal data;
   d) the basic structure of the file;
   e) types of personal data including file;
   f) data communications to recipients, if applicable;
   g) the transfer of data to third countries, if applicable;
   h) the services or units before which data subjects can exercise their rights;
   i) the applicable security measures, including by indicating discriminated access criteria, if applicable.

2. The legal provisions dictate the elimination of files must indicate the destination of the same or its data and the measures to be taken for its destruction.

ARTICLE 41
(Communication of data in the public sector)

Personal data processed by Public Administration bodies cannot indicate that they are communicated to other entities, bodies, services or others that have competence in different matters, except in the following circumstances.

a) such communication is permitted by legal provision or authorization by the Data Protection Agency;
b) the purpose of the communication is the further processing of data for historical or statistical purposes.

SECTION IX
Specific Provisions Applicable to Data Processing Personnel in the Private and Cooperative Sector

ARTICLE 42
(Applicable rule)

Data processing by the private and cooperative sectors is subject to:

a) the provisions of this law, with the exception of that contained in Section VIII;
b) the provisions of legislation specify that regulate the processing of personal data in certain sectors of activity.

ARTICLE 43
(File types)

The personal data files of private sector controllers include, among others. the following:

a) workers file;
b) occupational medicine file;
c) customer management file;
d) input and output file;
e) video surveillance file.

CHAPTER III
Data Protection Agency

ARTICLE 44
(Nature and composition)

1. Data Protection Agency is a legal person governed by public law. Endowed with legal personality. With administrative, financial patrimonial antinomy, who is responsible, namely:

   a) monitoring the application of the provisions of this law;
   b) issue recommendations, guidelines and instructions on best practices in the processing of personal data;
   c) issue an opinion on access to nominative documents;
   d) issue an opinion on the document classification system;
   e) to assess and decide on complaints addressed to it and guarantee the exercise of the right of access. Data rectification, updating and cancellation;
   f) register publish personal data file register;
   g) to guarantee the holders of personal data u obtain accurate information about their rights in the scope of processing and appropriate;
   h) guide the application of the necessary and appropriate technical and security measures;
   i) cooperate with international personal data protection authorities and supervise international movements of personal data;
   j) exercise its sanctioning function in terms of the protection of personal data, under the terms of this law;
   k) to prepare and forward annually to the Holder of the Executive Branch a report on the state of application of the present law and of my activity;
   l) issue an opinion on the application of this law and other complementary acts.

2. The Data Protection Agency is composed of seven members, designated as follows:

   a) three citizens appointed by the President of the Republic, of whom he appoints the President of the Agency;
   b) three citizens elected by the National Assembly;
   c) a Judicial Magistrate elected by the Superior Council for the Judiciary.

ARTICLE 45
(Organization and operation)

The organization and functioning of the Data Protection agency are established by a diploma from the holder of the Executive branch.

ARTICLE 46
(Code of conduct)

1. The Data Protection Agency encourages the creation of a code of conduct within the scope of data protection.

2. The participation of representatives of the right holders of the data in the preparation and application of codes of conduct is encouraged.

3. Codes of conduct must be registered with the Data Protection Agency.

4. The Data Protection Agency may reject the registration of codes of conduct when it considers them to be contrary to the provisions of this law and other applicable legislation.

5. It is up to the Data Protection Agency to issue opinions and recommendations so that the person responsible for creating the code of conduct can make the necessary corrections.

Chapter IV
(Administrative and Jurisdictional Protection)

SECTION I
(General depositions)

Article 47
(Administrative and Jurisdictional Protection)

1. Without prejudice to the right to complain to the Data Protection Agency, any person may, under the law, use administrative or jurisdictional means to ensure compliance with the legal provisions on the protection of personal data.

2. The decisions of the Data Protection Agency are subject to administrative litigation.

ARTICLE 48
(Civil liability in the processing of personal data)

Anyone who has suffered a moral or property damage due to improper use of personal data, has the right to demand redress for damages suffered through the courts, and the judge is responsible for grading the injury objectively.

SECTION II
(Misdemeanors and Fines)

ARTICLE 49
(Subsidiary law)

The sanctioning regime established in the present law does not prejudice the application of the sanctioning regimes in force in special legislation.

ARTICLE 50
(Duty omitted)

Whenever the misdemeanor results from the omission of a duty applicable to the processing of personal data, the application of the sanction and the payment of the fine do not exempt the offender from complying with it, whenever possible.

ARTICLE 51
(Misdemeanors and fines)

1. Without prejudice to other sanctions that may be applicable, it is a contravention punishable by fines in an amount equivalent to the notional currency indicated below:

    a) USD 75,000.00 to USD 150,000.00, in the case of:

        i) non-compliance with the obligations established in articles 14, 15, 16, 17, 20, 30, 31, 32, 32;
        ii) negligent non-compliance with the obligation to notify the Data Protection Agency or its compliance with the provision of false information or with non-compliance with the provisions of this law;
        iii) failure to comply with the order of the Data Protection Agency to cease access to open data transmission networks to officials who do not comply with the provisions of this law.

    b) USD 65,000.00 to USD 130,000.00, in case of non-compliance with the principles contained in articles 6 to 11, of not obtaining the consent of the data subject for processing, unless the circumstances that exempt, as for non-compliance with the provisions of articles 18, 19, and 21 to 24.

2. In the case of legal persons, companies and mere de facto associations, the misdemeanors provided for in the preceding paragraph are recorded at three times the respective limits.

3. Attempt and negligence are punishable.

ARTICLE 52
(Negligence and attempt)

1. Negligence is punished in the breaches provided for in point ii) of paragraph a) article 51 of the present law.

2. The attempt is always punishable in the misdemeanors provided for in article 51.

ARTICLE 53
(Application of fines)

1. The application of the fines provided for in the law is the responsibility of the Data Protection Agency.

2. The decision of the Data Protection Agency, after being approved by its responsible person, constitutes an enforceable title. if it is not challenged within the legal period.

3. The deliberations of the Data Protection Agency are public.

ARTICLE 54
(Recipe)

1. The amount of the amounts charged, as a result of the imposition of fines, reverts to the State and to the Data Protection Agency.

2. The fines to be applied by the Data Protection Agency must be periodically updated.

SECTION III
Crimes

ARTICLE 55
(Failure to comply with obligations relating to the protection of personal data)

1. Without prejudice to the other obligations regulated in the present law, a crime punishable by a penalty of pressure of 3 to 18 months or corresponding fine is incurred by those who:

   a) omit the authorization form to the Data Protection Agency;
   b) Provide false, information in the notification or in, requests for authorization for the processing of personal data, or in this proceed to modifications not allowed by the present diploma;
   c) promote or carry out an illegal interconnection of personal data;

d) after the deadline set by the Data Protection Agency has exceeded to comply with the obligations provided for in this law or subsidiary legislation, they do not comply.

2. The penalty is increased to double its limits when dealing with personal data referred to in articles 13 to 16 of this law.

ARTICLE 56
(Improper access)

1. Anyone who, without authorization, accesses personal data whose access is forbidden, incurs a crime punishable by imprisonment from 3 months to 2 years or a corresponding fine.

2. Without prejudice to the previous number, the improper access occurs when:

   a) it is achieved through violation of technical safety rules;
   b) it is possible for the agent or third parties to know personal data;
   c) has provided the agent or third parties with a patrimonial benefit or advantage.

3. Criminal procedure depends on a complaint.

ARTICLE 57
(Addiction or destruction of personal data)

1. Who. Without proper authorization, deleting, destroying, damaging, deleting or modifying personal data, rendering them unusable or affecting their ability to use, incurs a crime punishable by imprisonment from 18 months to 3 years or a corresponding fine.

2. The penalty is doubled in its limits if the damage done is particularly severe.

3. If the controller is negligent. the penalty is imprisonment up to 2 years or a corresponding fine.

Article 58
(Qualified disobedience)

1. Anyone who, after being notified for the purpose, does not interrupt, cease or block the processing of personal data is punished with a prison sentence of up to 3 years or a corresponding fine.

2. Without prejudice to the previous number, qualified disobedience is incurred, who:

a) refuse, without just cause, the collaboration that is specifically required by the Data Protection Agency;
b) do not proceed with the deletion, total or partial destruction of personal data;
c) do not proceed with the destruction of personal data, a beautiful period of conservation established.

ARTICLE 59
(Breach of the duty of secrecy)

1. Who, being obliged professional, under the law, without just cause and without due consent. Revealing or disclosing in whole or in part personal data is punishable by up to 18 months imprisonment or a corresponding fine.

2. Only a prison term of up to 2 years or a corresponding fine in the following cases:

   a) when the crime is committed by a public official or equivalent;
   b) when the information is revealed with the intention of obtaining any patrimonial advantage or other illegitimate benefit; or
   c) when the revealed information endangers the reputation, the time and consideration or privacy of the data subject's private life.

3. Outside the cases provided for in the preceding paragraph, criminal proceedings depend on a complaint.

ARTICLES 60
(Punishment of the attempt)

In the crimes provided for in the previous provisions, the attempt is always punishable by imprisonment of up to 6 months or a corresponding fine.

ARTICLE 61
(Accessory punishment)

1. In conjunction with fines applied, it can be ordered as an accessory:

   a) temporary or permanent prohibition of processing, blocking, payment or total or partial destruction of data;
   b) publicizing the condemnatory sentence;
   c) the public warning or censorship of the controller.

2. The publicity of the condemnatory decision is made: at the convict's expense, in the periodical publication of greater circulation, as well as through the posting of a public notice in an appropriate support, for a period of not less than thirty days.

3. The publication is made by extract containing the information elements and the sanctions applied, as well as the identification of the agent.

ARTICLE 62
(Infringement)

1. If the same fact constitutes both a crime and a misdemeanor, the agent is always punished with the title of crime.

2. The penalties applied to contraventions in competition are always cumulated materially.

CHAPTER V
Final provisions

ARTICLE 63
(Legalization of existing supports)

Data processing existing at the date of entry into force of this law must be notified to the Data Protection Agency within a maximum period of two years from the entry into force of this law.

ARTICLE 64
(Revocation)

All legislation that contradicts this law is revoked.

ARTICLE 65
(Regulation)

The present law must be regulated by the Executive, within one hundred and twenty days, counted from the date of its publication.

ARTICLE 66
(Doubts and omissions)

The doubts and omissions resulting from the interpretation and application of this law are resolved by the National Assembly

ARTICLE 67
(Implementation)

This law enters into force on the date of its publication.

It is analysed and approved by the National Assembly, in Luanda on the 24th May, 2011.

The Speaker of the National Assembly, António Paulo Kassoma.

It is enacted on the 8th June 2011.

It is Published.

The President of the Republic, JOSÉ EDUARDO DOS SANTOS

Resolution No. 14/11
of 17th June

Considering that the MPLA Parliamentary Group requested the movement of Deputies in the National Assembly, namely the cessation of deputy deputies' powers and the resumption of the mandate of Deputies in the National Assembly, in order to comply with the Constitution of the Republic of Angola and the Organic Law on the Functioning and Legislative Process of the National Assembly;

Considering that the request for the cessation of the powers of deputy deputies and the resumption of the seats of Deputies in the National Assembly obeys the requirements established in article 155 of the Constitution of the Republic of Angola and of paragraph 2 of article 7 of Law 6/93, of 4 June - Organic Law of the Members' Statutes;

The National Assembly approves by order of the people under the terms of paragraph i) of article 166 of the Constitution of the Republic of Angola the following resolution;

1. - The termination of the powers of deputies is approved:

   a) Filomena José Trindade, nº 152 on the list of the National Electoral Circle holding the Voter Card nº 690 960 230;
   b) Maria Teresa de Jesus António Komba, No. 153 on the list of the National Electoral Circle, holder of Voter Card No. 1 411 360 281.

2. - The resumption of seats and integration in the Permanent Work Committees in the National and Friendship Groups of the National Assembly is proven, as the reasons that led to the provisional suspension of the mandate of Deputy of the following Deputies ceased:

   a) Vitoria Francisco Correia da Conceição nº 105 from the National Electoral Circle list, holder of Voter Card nº 17 683 560 495, which joins the Health, Environment, Family, Childhood and Promotion of Women Commission, the National Group of the Forum of Parliaments of the Community of

Portuguese Speaking Countries (CPLP) and the Friendship Group of Central and South America;

b) Francisca de Fátima do Espirito Santo de Carvalho, number 79 on the list of the National Electoral Circle, holder of Elector Card No. 10 938 860 235, who joins the Committee on Education, Science and Technology, Cultural, Youth, Sports, Affairs Religious and Social Communication: the National Group of the Forum of Parliaments of the Community of Portuguese Speaking Countries (CPLP) and the Friendship Group of Central and South America.

3. - This resolution enters into force immediately.

It is analysed approved by the National Assembly, in Luanda on May 24, 2011.

It is Published.

The Speaker of the National Assembly, António Paulo Kassoma.