

**OFFICIAL PART**

**PRESIDENTIAL ACTS**

**OFFICE OF THE PRESIDENT OF THE REPUBLIC**

LAW No. 2013-450 dated June 19, 2013 on the protection of personal data. THE NATIONAL ASSEMBLY has adopted, the President of the Republic promulgates the law which content as follows:

**CHAPTER I**

Definition

**First Article.**- Definitions of legal instruments of ECOWAS, the African Union or the International Telecommunication Union prevail for terms not defined in this Act.

For the purposes of this Act the following terms mean:

- -Cryptology activity , any activity aimed at the production, use , import, export or sale of cryptology ;
- Approval , formal recognition by an authorized organization that the evaluated product or system can protect up to a specified level ;
- Secured Electronic Archiving, all terms of conservation and management of electronic records to guarantee their legal value for the duration necessary;
- - Violation of human dignity, infringement , except in cases of attempt on the life , physical integrity or freedom , which has important effect to treat the person as a thing, as an animal or as a being which would be denied any right;
- Protection Authority , the independent administrative body to ensure that the processing of personal data are implemented in accordance with the provisions of this Law;
- Encryption , any technique which transforms digital data into an unreadable format using cryptology ;
- Code of conduct, terms of use developed by the controller in order to achieve proper use of IT resources, the Internet and electronic communications structure concerned and approved by the Authority for protection;
- Electronic commerce , economic activity in which a person offers or provides , distance and by electronic means , the supply of goods and provision of services; meaning also in the field of electronic commerce, the activities of provision of services such as consisting in providing online information , commercial communications , research tools , access and retrieval of data, access to a communication network or hosting of information, even if they are not remunerated by those who receive them ;
- Electronic communication, any emission, transmission or reception of signs , written materials, images, sounds or videos by electromagnetic , optical or other means ;

- -Consent of the concerned person , any express manifestation of will , unequivocal , specific and informed free by the person concerned or his legal representative , legal or conventional agrees that his personal data are subject to manual or electronics processing;
- Secret Conventions , any unpublished key necessary for the implementation of a medium or of the provision of encryption for cryptographic operations ;
- E-mail , all messages in the form of text, voice, sound or image sent over a public communications network , stored on a server in the network or in the recipient 's terminal equipment until the latter recovers ;
- Cryptography , the science related to the protection and information security including confidentiality, authentication, integrity and non-repudiation ;
- Cybercrime , any criminal offense that is committed by means of a network or a computer system or electronic communications;
- Recipient of processing of personal data , any person entitled to receive a communication of such data , other than the concerned person, the responsible person of processing, the subcontractor and the persons who, due to their duties, are responsible for the processing of data ;
- Document, the result of a series of letters, characters , numbers , figures, or any other signs or symbols in an intelligible meaning, regardless of media and transmission terms ;
- Personal data means any information of any kind and regardless of media , including sound and image related to an identified or identifiable directly or indirectly, by reference to an identification number or to one or more specific cultural, social and economic factors specific to his physical , physiological, genetic , psychological identity;
- Computer data or data , any representation of facts , information or concepts in a form suitable for computer processing , including a program suitable to perform a function by an information system ;
- Data relating to subscribers , any information in the form of computer data or any other form that is held by a service provider and relating to subscribers of its services other than traffic data , content , and permitting to establish on the basis of a contract or arrangement services;
- The type of communication service, the technical provisions taken thereto and the period of service;
- The identity , the postal or geographic address, telephone number or other access number , information about the location , billing and location where communications equipment is;
- Traffic data , all data relating to a communication by an information system , produced by the latter as a feature of the chain of communication , indicating the origin , destination, route, time , date, size and duration , or type of underlying service ;
- Sensitive data, all personal data concerning opinions or religious activities , philosophical, political , union , sexual or radical life, health, social measures , prosecution , criminal or administrative sanctions;
- Exchange of computer data(EDI ) , all electronic transfer of information from one electronic system to another implementing a standard agreed by organizing information ;

- Written materials, any sequence of letters, characters , numbers or any other sign or symbol that has an intelligible meaning , whatever their report and the transmission format;
- Personal data File, any structured set of accessible data according to criteria determined that whether this set is centralized , decentralized distributed on a functional or geographical basis to identify a particular person;
- Service Provider, any corporation that provides public electronic communications services or IT services ;
- Information, any element of knowledge likely to be represented through conventions to be used , stored , or communicated . The information can be expressed in written form, visual, aural , digital, etc. . ;
- Critical Infrastructure , physical facilities and information technology , networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health , safety or economic and social welfare of citizens or the continued operation of state services ;
- Interconnection of personal data, any connecting mechanism consisting in connecting data processed by a determined purpose with other data processed for the same purpose or not or linked by one or more data controller ;
- E-mail, any information generated, sent, received or stored by electronic , optical or similar means including, but not limited to , electronic data interchange ( EDI) , electronic mail, telegram , telex and the fax.
- Minor means any person under the age of eighteen years , in accordance with the Criminal Code;
- Means of cryptology, all scientific and technical tools (hardware or software) that are used to encrypt and / or decrypt , it is also meant , , by means of encryption hardware or software designed or modified to transform data that it is whether written or signals using secret agreements or to realize the inverse operation with or without a secret agreement ;
- - Third party countries , all ECOWAS non-member state;
- Concerned Person means any natural person who is the subject of processing of personal data ;
- Provision of cryptology, any operation aiming at the implementation on oneself behalf or others , means of cryptology ;
- Cryptology Service provider , any individual or entity that provides a service of cryptology ;
- Child Pornography , all data regardless of the nature or form that visually depicts a child under 18 years of age engaged in sexually explicit conduct or images depicting a child under 15 years engaged in behavior sexually explicit ;
- Direct prospecting , sending messages , regardless of the media or particular commercial, political or charitable nature, designed to promote, directly or indirectly, the goods , services or image of a person selling goods or providing services;
- Racism and xenophobia in ICT , any written material, picture or other representation of ideas or theories, which advocates , promotes or incites hatred, discrimination or violence against a person or

group of persons because of race , color , descent or national or ethnic origin or religion, insofar as it serves as a pretext for one or the other of these elements or that incites such acts ;

- Person Responsible for processing , natural or legal persons, public or private , any other organization or association which alone or jointly with others decides to collect and process personal data and determines the purposes ;
- Electronic signature, any data that results from the use of a reliable identification ensuring its link with the act to which it is attached ;
- SMS, English acronym meaning " Short Message Service " ;
- Subcontractor , any person or entity , public or private, any other organization or association that processes data on behalf of the person responsible for processing ;
- Monitor , any activity involving technical or electronic means to detect , observe , copy or record the movements , images, words, written material , or the state of an object or a person fixed or mobile ;
- Information system or computer system , any single device or not , any set of interconnected devices in all or part of an automated data processing program execution ;
- Third Party , any natural or legal person, public or private , any other organization or association other than the data subject, the person responsible for the processing , the subcontractor and the persons who, under the direct authority of the person responsible for processing or the processor, are authorized to process the data;
- Processing of personal data means any operation or set of operations performed or not by automated processes or not , and applied to data, such as the collection, processing , recording , organization , backup, copy , consultation , use, disclosure by transmission , dissemination or otherwise making available , alignment or combination, blocking, encryption, erasure or destruction of personal data .

## **CHAPTER 2**

Purpose and scope of the Permanent Secretary of the National Commission of the Global Environment Facility.

**Art. 2.** – The hereby law has as purpose to govern the protection of personal data.

**Art. 3.** – Are subject to the provisions of this Law:

Any collection, treatment , transmission, storage and any use of personal data by a natural person , the state , local authorities , and public or private corporations;

Any automated processing or not of data included or intended to be included in a file;

Any data processing implemented on the national territory;

All processing of data concerning public security, defense, investigation and prosecution of criminal offenses or the state security, subject to the exceptions defined by the specific provisions set by other legislation in force.

**Art. 4.** – Are excluded from the scope of this Law :

Data processing implemented by an individual in the exclusive context of personal or household activity , provided that the data are not intended for systematic communication to third parties or dissemination ;

Temporary copies made in the course of technical transfer of activities and access to a digital network supply for automatic, intermediate and transient data and the sole purpose of allowing other recipients of the service the best access possible to the transmitted information.

### CHAPTER 3

Formalities necessary for the processing of personal data

**Art. 5** – The treatment of personal data is subject to prior notification to the personal data protection body.

The statement includes a commitment that the processing meets the requirements of the law.

The protection body shall issue a receipt in response to the statement, if any, electronically. The applicant may implement the processing upon receipt of its receipt, he is not exempted from any of his responsibilities.

The processing falling under the same organization and the same or interrelated goals may be a single statement. The information required under the declaration are provided for each of the processing to the extent they are his own.

**Art. 6** – are exempted from the formalities statement :

The data processing used by an individual in the exclusive context of his personal, domestic or family activities;

The processing of data relating to an individual which publication is prescribed by law or regulation;

Data processing whose sole purpose is the keeping of a register which is intended for private use only;

The processing of data for which the responsible person designated a correspondent for the protection of personal data in charge of ensuring in an independent manner, the compliance with the obligations provided for in this Law except where a transfer of personal data to a third country is considered.

**Art. 7** – are subject to prior authorization by the data protection body before implementation:

The processing of personal data relating to genetic, medical data and scientific research in these areas;

The processing of personal data on data relating to offenses, convictions or security measures imposed by the courts;

Processing on a national identification number of the same nature, such as telephone numbers;

The processing of personal data with biometric data

The processing of personal data having a pattern of public interest, particularly for historical, statistical or scientific purposes;

The transfer of personal data considered to a third country.

The application for authorization shall be submitted by the responsible person of the processing or his legal representative.

The authorization does not relieve the responsibility to third parties.

**Art. 8** – for the most common categories of processing of personal data including those implementing is not likely to adversely affect the privacy or freedoms, the protection body prepares and publishes standards and procedures designed to simplify or to relieve the responsible person from the obligation of prior notification .

**Art. 9** – the request for an opinion , the statement and the application for authorization is sent to the data protection body and shall contain at least the following information:

- The identity, postal or geographic residence address of the responsible person of the processing or if it is not established in the country, those of his duly authorized representative, and in the case of a person morality, its name , its headquarters , the identity of the legal representative 's registration number in the trade register, the tax payer account number;
- The purpose (s) of processing and the general description of its functions;
- The interconnections considered in all other forms of linkage with other processing;
- The personal data processed, their origin and the categories of persons affected by the processing;
- The shelf life of processed data;
- The service (s ) responsible for implementing the processing and the categories of persons who, due to their duties or for the needs of the service, have direct access to the data collected ;
- The recipients authorized to receive processed data;
- The function of the person or department to which is exercised the right of access;
- The measures taken to ensure security of the processing, protection and confidentiality of data processed;
- The indication for a subcontractor or transfer of personal data to a third country.

In case of change in the particulars listed above, the person responsible for the processing shall inform without delay the national body for the protection of personal data.

The conditions of submission of the application for authorization and procedures for granting authorizations are established by decree of the Cabinet Meeting.

The protection body may by decision require the additional conditions of submission of the application for authorization or statement and authorization granting procedures.

**Art. 10-** The statement or request for authorization may be made to the protection body by email, post or by any other means of delivery against acknowledgment of receipt.

**Art. 11 –** The Protection Body shall make a decision within one month from the receipt of the statement or request for authorization. However, this period may be extended to another month upon reasoned decision of the protection body.

The lack of response of the data protection body within the time limit is equivalent to a rejection of the statement or request for authorization. In this case, the responsible person of the processing may appeal to the competent court.

The procedure for making statements or granting authorizations for the processing of personal data in accordance with the provisions of this Act are set by decree.

**Art. 12 –** The correspondent to the protection of personal data is a person enjoying qualifications to perform such missions. He keeps a list of the processing performed immediately accessible to anyone upon request and cannot be subject to any sanction on the part from the employer, because of the performance of his tasks. He can size the data protection body for the difficulties encountered in the performance of his duties.

The designation of the correspondent by the responsible person of the processing is notified to the data protection body. It is also noticed, as appropriate to the staff representative authorities.

The Profile and conditions of remuneration corresponding to the protection of personal data are subject to a decision of the Minister of Information and Communication Technologies, upon proposal from the Protection Body.

In case of failure observed in his duties, the correspondent is responsible for the corresponding functions on demand, or after consultation, of Protection Body.

**Art. 13 –** The processing of personal data carried out on behalf of the State, a public or private legal entity managing a public service authorized by decree, after reasoned opinion of the Data Protection Body.

These processing include:

- The state security, national defense or public security;
- The prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal convictions or security measures;
- The census of population;
- The processing of wages, pensions, taxes and other liquidations.

## CHAPTER 4

### *Guidelines for the processing of personal data*

**Art. 14** – The processing of personal data is considered legitimate if the person concerned gives his express consent.

However, there may be exceptions to this requirement of consent when the responsible person of the processing is duly authorized and the processing is necessary;

- Either for the compliance with a legal obligation to which the responsible person of the processing is subject;
- or for the execution of a task in the public interest or in the exercise of official authority vested in the responsible person of the processing or the third party to whom the data are disclosed;
- or for the execution of a contract to which the concerned person is a party or the execution of pre-contractual measures taken in the application;
- or for safeguarding the interests or fundamental rights and freedoms of the concerned person;

**Art. 15** – The collection, recording, processing, storage, transmission and file interconnection of personal data must be made in a lawful and fair manner.

**Art 16** – the data must be collected for specified, explicit and legitimate purposes and cannot be further processed in a way incompatible with its aims.

They must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed.

They must be kept for a period that does not exceed the period necessary for the purposes for which they were collected or processed.

Beyond the period required, the data can be subject of a conservation only for responding specifically to processing for historical, statistical or research purposes under the law.

**Art 17** – The collected data must be accurate and, where necessary, kept up to date.

All reasonable measures shall be taken to ensure that inaccurate or incomplete data, with regard to the purposes for which they were collected and subsequently processed, are erased or rectified.

**Art 18** – The principle of transparency requires a mandatory and clear information from the responsible person on the processing of the personal data.

**Art 19** – The personal data must be processed confidentially and shall be protected especially when the processing of these data include transmission of data over a network.

**Art 20** – When the processing of personal data is carried out on behalf of the person responsible for the processing, he must choose a subcontractor providing sufficient guarantees for the protection and privacy of data security.

It is the responsibility of the person responsible for the processing as well as the sub-contractor to ensure compliance with this Law.

**Art 21** – Is prohibited and punishable by a term of imprisonment of ten to twenty years and a fine of 20 million to 40 million CFA francs, the proceeds made from the collection and any data processing revealing racial , ethnic or regional affiliation , political opinions , religious or philosophical beliefs,

trade union membership, sex life, or more generally, those genetic data on the health of the person concerned .

This prohibition is not applied:

- When the processing of personal data relates to data which are manifestly made public by the concerned person;
- When the processing of genetic or related to the health data is necessary to protect the vital interests of the person concerned or another person in the case where the person concerned is physically or legally incapable of giving his consent;
- When processing, namely genetic data, is necessary for the establishment, exercise or defense of a legal claim of the person concerned;
- When a judicial proceeding or a criminal investigation is opened. In this case, the processing of personal data is prosecuted for the determination of the facts or the manifestation of the truth;
- When the processing is done within the legitimate activities of a foundation, association or any other non-profit organization with a political, philosophical, religious, fraternal or union goals. However, the processing must be related only to members of this body or to persons with one regular contacts related to its purposes and that the data are not disclosed to third parties without the consent of the persons concerned.

All these cases of processing of personal data are authorized and supervised in their design and implementation by the protection body.

**Art 22** - Is prohibited and punishable by imprisonment for one to five years and a fine of 1 million to 10 million CFA francs , direct marketing using all means of communication using , in any form whatsoever, the personal data of an individual who has not expressed his consent to receive such surveys character .

**Art 23** – the processing of personal data carried out for purposes of journalism, expression research, artistic or literary is recognized when it is implemented solely for literary and artistic expression or exercise , as professional, business or journalism researcher, in compliance with the ethical rules of the profession.

**Art 24** - The provisions of this Law shall not preclude the application of provisions of the law relating to print or audiovisual sector of the Criminal Code which stipulate the conditions for exercising the right of reply and prevent , limit , repair and , if appropriate, penalizing offenses against privacy and reputation of individuals.

**Art 25** - No any court decision involving an assessment of the behavior of an individual can be based on automated processing of personal data intended to evaluate certain aspects of his personality.

No any administrative or private decision involving an appraisal of human behavior can be based solely on automated processing of personal data which describes the profile or personality of the individual.

**Art 26** - the person responsible for the processing can be allowed to transfer personal data to a third country only if the state provides a higher level of protection or equivalent privacy, freedoms and fundamental rights of individuals with regard to the processing which the data are or may be subjected.

Before any actual transfer of personal data to that third country, the person responsible for the processing must first obtain the permission of the Protection Body .

The transfer of personal data to third countries is subject to regular monitoring of the data protection body in light of their purpose

**Art 27** - The interconnection of files is authorized only if it permits to achieve legal and statutory objectives with legitimate interest to those responsible for the processing.

It cannot lead to discrimination or reduction of rights, freedoms and guarantees for the persons concerned or subject to inappropriate security measures and take into account the principle of relevance of the data subject of the interconnection.

## CHAPTER 5

### Rights and exceptions to the rights of the person concerned

**Art 28** - The person responsible for the processing shall provide the person whose data are being processed, at the latest, during the collection and whatever the means and media used , with the following information:

- His/her identity and, if applicable, his/her authorized representative;
- The purpose (s ) set for which the data are intended;
- The categories of data concerned;
- The recipient (s) to whom the data might be disclosed;
- The possibility of refusing to appear on the file in question;
- The existence of a right of access to data concerning the person and the right to rectify any such data;
- The shelf life of the data;
- The possibility to transfer the data to third countries.

**Art 29** - Any person whose personal data are being processed may request in the form of questions and obtain from the person responsible for this processing;

- Information permitting to know and challenge the processing;
- Confirmation that personal data relating to him are or are not subject to this processing;
- The communication of personal data concerning them and of any available information as to the origin thereof;
- Information about the purposes of the processing, the categories of personal data processed and the recipients or categories of recipients to whom the data are disclosed.

If unable to access, the person concerned, right of access can be exercised by the data protection body that has a power of investigation in the matter and may order the rectification, erasure or blocking of data the processing of which does not comply with this Law.

The data protection body shall inform the person concerned of the results of its investigations.

The person responsible for the processing can be opposed to the grossly unfair requests from the same person, including their number, repetitive or systematic character. In case of dispute, the

burden of patent unreasonableness of requests is the responsibility of the person responsible for the processing to whom they are addressed.

**Art 30** – any person concerned has the right:

- To oppose, on legitimate grounds relating to his/her particular situation that the personal data relating to him/her being processed, unless legal provisions expressly providing the processing. In case of a legitimate objection, the processing implemented by the person responsible for the processing may not be related to the data in question;
- To oppose, on demand and without charge, to the processing of data relating to prospecting purposes;
- To be informed before personal data relating to him/her be disclosed for the first time to third parties or used on behalf of third parties for prospection and to be expressly granted the right to object free of charge to the aforesaid disclosure or use .

**Art 31-** Any person, proving his/her identity may require the person responsible for the processing that be, as appropriate , rectified, completed, updated , deleted or locked the personal data relating to him/her which is inaccurate, incomplete, ambiguous , outdated or whose collection, use , disclosure or storage is prohibited .

**Art 32-** Ration of the Permanent Secretary of the National Commission of the Global Environment Facility.

The successors of a deceased person proving their identity may, if the evidence brought to their knowledge let them assume that the personal data concerning them being subject of processing have not been updated , require the person responsible for this processing take into account the death and make the updates that must be the consequence .

When those successors request for that, the person responsible for the processing must justify , free of charge for the claimant , that he has made the operations required under the preceding paragraph.

**Art 33-** The person concerned has the right to obtain from the person responsible for the processing the erasure of personal data and on the termination of the distribution of such information , particularly with regard to the personal data that the person concerned was made available when he was a minor , or for one of the following reasons :

- Data is no longer necessary for the purposes for which it was collected or subsequently processed;
- The person concerned has withdrawn the consent on which the processing was based or when the authorized shelf life has expired and there is no other legal ground for the data processing;
- The person concerned objects to the processing of personal data concerning him/her when there are no legal grounds of the aforesaid processing;
- Data processing does not comply with the provisions of this Law;
- For any other legitimate reason.

**Art 34-** When the person responsible for the processing has made public the personal data of the person concerned, he/she shall take all reasonable steps, including technical measures, with regard to the data released under his/her responsibility, to inform the third parties which are processing the

aforesaid data that a concerned person asks them to remove all links to these personal data, or any copy or reproduction thereof.

When the person responsible for the processing has authorized a third party to publish the personal data of the concerned person , he/she is deemed responsible for this publication and shall take all appropriate measures to implement the right to digital oblivion and erasure of personal data .

**Art 35-** The person responsible for the processing shall carry out the erasure without delay, unless the conservation of personal data is required:

- Either for the right to freedom of expression;
- or for reasons of general interest in the field of public health , in accordance with the law;
- or for the sake of compliance with a legal obligation to keep personal data under the legislation to which the person responsible for the processing is subject.

**Art 36-** The person responsible for the processing shall establish appropriate mechanisms to ensure the implementation of the rule of right to digital oblivion and to erasure of personal data or periodically review the need to keep data in accordance with provisions of this Law.

When the erasure is completed, the person responsible for the processing shall not perform any further processing of such personal data.

**Art 37-** The Data Protection Body shall adopt measures and guidelines for the purposes of specifying:

- The conditions for the removal of links to these personal data, copies or reproductions thereof existing in electronic communication services publicly available;
- The conditions and criteria applicable to the limitations of the processing of personal data.

**Art 38-** When the personal data are subject to automated processing in a structured format and commonly used , the person concerned has the right to obtain from the person responsible a copy of the data undergoing processing automated in a structured electronic format that is commonly used and allows reuse of these data by the persons concerned.

When the person concerned has provided the personal data and the processing is based on consent or a contract, he/she has the right to forward these personal data and any other information he/she provided and which are kept by an automated processing system to another system in a circuit diagram which is commonly used without the person responsible for the processing to whom the personal data are removed precludes it.

The Data Protection Body may specify the electronic format, as well as technical standards, methods and procedures for the transmission of personal data.

## **CHAPITRE 6 :**

### **Duties of Officers and their subordinates**

**Art 39-** The processing of personal data is confidential. It is performed only by persons acting under the authority of the person responsible for the processing and only on his instructions.

**Art 40-** The processing of personal data is confidential. It is performed only by persons acting under the authority of the person responsible for the processing and only on his instructions.

Art 40 - The person responsible for the processing shall take all precautions with regard to the nature of the data and especially, to prevent it from being distorted, damaged, or that unauthorized parties have access.

When the processing is implemented on behalf of the person responsible for the processing, he/she chooses a subcontractor that provides sufficient to meet the technical and organizational security measures relating to the processing performed. It is the responsibility of the person responsible for the processing as well as sub-contractor to ensure compliance with those measures.

**Art 41-** he person responsible for the processing shall:

- prevent any unauthorized person from having access to the installations used for data processing;
- prevent data media from being read, copied, modified or removed by unauthorized persons;
- prevent the unauthorized introduction of any data in the information system, and unauthorized inspection, modification or deletion of recorded data;
- prevent data processing systems from being used for money laundering and terrorist financing;
- Ensure that when using an automated data processing system, authorized persons do not have access to data under their authority;
- Ensure that the identity of parties to whom the data may be transmitted by transmission facilities; can be verified and ascertained
- Ensure that posteriori identity of persons having access to information containing personal data system , the nature of data that have been introduced , modified, altered , copied, deleted or read in the system, the time at which the data were manipulated can be verified and established a ;
- prevent data from being read , copied, modified, altered or erased in an unauthorized manner, when releasing data and transporting support ,
- Save the data by creating backup copies for security protection. The person responsible for the processing must implement all technical measures and appropriate organization to protect data he/she processes against accidental or unlawful destruction or accidental loss, alteration, disclosure or unauthorized access in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

**Art 42-** The person responsible for the processing is required to prepare an annual report for the data protection body on compliance with the provisions announced in Article 41 of this law.

**Art 43-** The personal data are kept for a period fixed by the data Protection Body according to the goals of each type of processing for which they were collected in accordance with applicable laws.

**Art 44-** The person responsible for the processing shall take all appropriate measures to ensure that personal data processed can be exploited regardless of the support used.

**Art 45-** shall be punished with imprisonment from one month to two years and one million to 10 million CFA francs fine whoever obstructs the data Protection Body:

- Either by opposing the exercise of the tasks entrusted to its members or authorized agents in accordance with the provisions of this Act;
- Or by refusing to disclose to its members or authorized agents, information and documents necessary for their mission, or concealing such documents or information, or making them disappear;
- Or by providing information that is not consistent with the content of the records as it was at the time the request was made or does not present this content in a directly accessible form .

The prosecutor or the competent investigating judge is informed without delay of the barriers to actions of the data Protection Body and shall take all appropriate measures to withdraw them and prosecute the perpetrator or accomplice.

## **CHAPTER 7**

### **The personal data protection Body**

**Art 46-** The mission of the personal date Protection Body is entrusted to the independent administrative body responsible for the regulation of Telecommunications and Information and Communication Technologies.

In this regard, the Protection Body shall ensure that processing of personal data be implemented in accordance with the provisions of this Law and its implementing regulations.

**Art 47 –** The data Protection Body ensures that the use of Information and Communication Technologies shall not affect or does not include a threat to freedom and privacy for users located throughout the national territory.

In this capacity, it is responsible for:

- informing the persons concerned and the officers handling of their rights and duties;
- responding to any request for advice on processing of personal data;
- Establishing an by law that spell out the rules relating to the proceedings, the investigation and presentation of cases;
- receiving reports and granting authorizations for the implementation of personal data processing, or withdrawing them as provided by this Law;
- receiving claims and complaints relating to the implementation of personal data processing and informing authors of the subsequent outcome given thereof;
- informing without delay the competent judicial authority of the offenses of which it was informed in the course of its missions;

- Determining the necessary guarantees and appropriate measures for the protection of personal data;
- carrying out, through sworn officers, audits on all personal data processing;
- imposing administrative and pecuniary penalties against persons responsible for the processing who fail to comply with the provisions of this Law;
- Updating and making available for public consultation a directory of personal data processing;
- Consulting people and organizations that process personal data or carry out or tests or make experiences in the matter;
- giving its opinion on any legal bill in relation to the protection of freedom and privacy;
- Developing guidelines for the processing and protection of personal data;
- participating in scientific research, training and study in relation to the protection of personal data, and in general, freedoms and privacy;
- authorizing certain conditions set by decree of the Cabinet Meeting cross-border transfers of personal data ;
- making proposals likely to simplify and improve the legislative and regulatory framework governing the processing of personal data ;
- establishing mechanisms of cooperation with the bodies in charge of protecting personal data from other countries;
- participating in international negotiations on the protection of personal data ;
- Establishing and implementing an annual activity report to the President of the Republic and President of the National Assembly.

**Art 48** – the cryptologic service provider cannot object the Protection Body, professional secrecy to which it is submitted in accordance with legal and contractual provisions.

The person responsible for the processing acting in the course of performing his/her duties cannot object the Protection Body of professional secrecy to which it is subject .

**Art 49** – The Protection Body may impose in respect of person responsible for processing the following measures:

- A warning to the person responsible for processing who fails to comply with obligations under this Law;
- A formal notice to stop the deficiencies observed in the specified time.

**Art 50** – when the implementation a personal data processing leads to a violation of human freedoms the Protection Body after an adversarial procedure , shall decide the:

- Interruption of the implementation of the processing;
- locking of some personal data processed;

- temporary or permanent prohibition of a processing contrary to the provisions of this Law.

**Art 51** – The Protection Body may, after hearing the person responsible for the processing or his subcontractor who fails to comply with the provisions of this Law and the notice that was sent to him , pronounce against him, the following sanctions:

- The temporary withdrawal of the authorization;
- The final withdrawal of the authorization;
- A financial penalty.

The amount of the penalty is proportionate to the seriousness of the breaches committed and the benefits derived from the breach.

The amount of the penalty may not exceed the sum of 10 million CFA francs.

In case of repeated failure within five years from the date the penalty previously imposed becomes final and cannot exceed 100 million CFA francs or in the case of a company, it cannot exceed 5% of the turnover excluding tax of the last financial year to a maximum of 500 million CFA francs.

These administrative and financial penalties are applied without prejudice to criminal penalties.

**Art 52** – the procedures for withdrawal of authorization and collection of the penalty are set by decree.

## CHAPTER 8

### Provisional and final provisions

**Art 53-** the persons in charge of the processing of personal data have a period of six months from the date of entry into force of this Law, to comply with its provisions.

**Art 54** – the hereby law will be published in the Official Gazette of the Republic of Cote d'Ivoire and enforced as State law.

Issued in Abidjan, on June 19, 2013.

\_\_\_\_\_ Alassane OUATTARA