

REPUBLIC OF BENIN

---

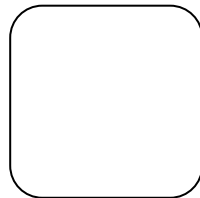
NATIONAL COMMISSION OF INFORMATION (FREEDOM) AND PRIVACY

---



---

LAW N° 2009-09 OF MAY 22, 2009



# Table of Contents

<b>Chapter I one : Principles and Definitions .....</b>	<b>3</b>
<b>Chapter II : Conditions of Processing Personally Identifiable Information ...</b>	<b>5</b>
<b>Chapter III : Individuals' Rights with Regard to the Personally Identifiable Information .....</b>	<b>8</b>
<b>Chapter IV : Commission in Charged of the Protection of Personally Identifiable Information and processing verification/Controle.</b>	<b>10</b>
<b>Chapter V : Obligations of the Processing Officers .....</b>	<b>18</b>
<b>Chapter VI: Conditions of Sanctions and Final Dispositions.....</b>	<b>21</b>

**REPUBLIC OF BENIN**

**THE GOVERNMENT OF THE REPUBLIC OF BENIN**

**LAW N° 2009-09 OF MAY 22, 2009**

**Dealing with the protection of Personally Identifiable Information (PII)  
in the Republic of Benin.**

The National Assembly considered and adopted/voted during its session of April 27, 2009.

Further to the Decision of Conformity to the Constitution DCC 09-064 of May 19, 2009 of the Constitutional Court,

The President of the Republic promulgates the law/act which states the following:

**CHAPTER ONE:  
PRINCIPLES AND DEFINITIONS**

**ARTICLE I  
PRINCIPLES**

**Section One(1)**: The present law/act applies to the digital processing of personally identifiable information, contained or to be displayed(inserted) in digital files, entirely or partially, or in manuals.

**Section Two(2)**: Information Science is to serve the humankind, it should not harm the human identity, the privacy of an individual, the human rights, the public, individual and collective liberties.

**Section Three(3)**: Any personal identification mechanism based on nominative, personal and biometric information collected from biometric records and finger

prints processed by means of appropriate technologies and attribution(issuance) of a unique National Identification Number, is managed by the provisions of the present law/act.

**Section four ( 4)**: According to the present law, it's meant that:

- Personally identifiable information: refers to any information that can identify, distinguish or trace any specific individual or susceptible to be, linked or linkable, such as an identification number or to one or different elements that are particular to that individual. The identification is made with the medium available or one that can be accessible to, the responsible of the processing or any other person;
- Personally Identifiable Information records: Any structured and stable set of personally identifiable information, accessible according to determined criteria;
- Person concerned with processing personally identifiable information: Refers to any individual whose information processed are related;
- Person in charge of the processing of Personally Identifiable Information: Refers to the individual, the public authority, the office or the entity that determines its finalities and its means;
- Subcontractor: refers to any person processing personally Identifiable Information on the behalf of (or under) the person in charge or responsible of the processing;
- Automated or digital Information Processing: A set of acquisition activities carried out by an automated medium-Information Technology (IT Systems)-, dealing with the information collection, recording, elaboration, the modification, storage, destruction, display, transmission and, in a general, their management;

- Processing Personally Identifiable Information: Refers to any activity or set of activities dealing with such information regardless of the medium used, including the acquisition, storage, organisation, consecration, adaptation or modification, extraction, consultation, management, communication by transmission or circulation to any other kind of releasing, reconciling and interconnecting, as well as the locking, obliteration or destruction;
- National Commission of Information Privacies NCIP: An organism of personally identifiable information protection and processing control.

**CHAPTER II**  
**PERSONALLY IDENTIFIABLE INFORMATION PROCESSING CONTROL**  
**CONDITIONS**

**Section Five 5:** Processing personally identifiable information only deals with information applicable to the following conditions:

- a. Be collected and processed in a loyal and permissible manner;
- b. Be collected for specific objectives, explicit, legitimate not fraudulent;
- c. Not subsequently processed in an incompatible manner with reference to the specified objectives;
- d. Be appropriate, relevant and non excessive with reference to the objectives for which they are collected and their subsequent processing;
- e. Be precise, complete and, if necessary, updated. Appropriate measures should be taken for the non precise or incomplete information, referring to the objectives for which they are collected or processed, be deleted or corrected;

- f. Be secured or stored in a practical way that makes the identification of subject individuals an easy task in a timely deadline possible to meet the objectives for which they are collected or processed.

The acquisition or the processing of information in any fraudulent, disloyal, illicit ways is forbidden.

Section 6: It is forbidden, unless full consent of the subject individual, to collect or process personally identifiable information which display, directly or indirectly, the racial or ethnic origins, the political opinions, philosophical or religious, the union groups that individuals belong to or health related and sexual life of such individuals.

However, the religious congregations or religious, philosophical, political or union groups may keep digital loggins orenrolments of their member or their correspondants. No control may therefore be carried against them.

For public Interest reasons, an exception may only be made to the above interdiction upon proposition or certified notice from the NCIP on provision made in the section 19 of the presente law.

Section 7: As the processing objectives requires it for certain categories of information, the interdiction in the preceeding section is not applicable to:

- a. The processings for which the subject individual gave his full consesnt, unless if the provisions of the present law in its section 6 does not allow the exercising of the interdiction even with the consent of the subject individual;
- b. The vital processings for the safeguarding of human life, for which the subject individual cannot give his consent as result of any legal inability or materialistic incapability;
- c. The processings initiated by an association or any other non profit religious, philosophical or union organisms /entities which goal is to manage their members or the management of individuals that interact with them on a regular basis during their day to day activities;

- d. The vital processings for a verification, a discharge or the defense of a legal right;
- e. The processings that are carried toward, the research in the medical health field.

Section 8: The personally identifiable information related to infringements, condemnations/convictions/judgements and to security measures may only be dealt by:

- a. The jurisdictions, the public authorities and moral individuals that manage a public office in the scope of their statutory/legal functions;
- b. The representatives of law, for the strict needs of their missions as they are assigned by the law;
- c. The other moral individuals, for the strict management needs of infringements related conflicts of which they are victims.

Article 9: The responsible of a personally identifiable information can only transfer the data to a Foreign Government if the subject country warranties sufficient degre of privacy, liberty and unalienable rights protection of the subject individuals that such data identify.

The degre of protection warrantied by a foreign country is evaluated based on the protection measures enforced in the very foreign Country, the security measures enforced in it, clear definition of the processing details such as its motivation, period/length as well as the nature, the origin and the destination of the processed data.

**CHAPTER III**  
**INDIVIDUALS' RIGHTS WITH REGARD TO THE PERSONALLY IDENTIFIABLE**  
**INFORMATION**

Section 10: Any individual has the right to oppose, for legitimate reasons, to the processing of its personally identifiable information.

Section 11: Any individual has the right to oppose, without any duty, to the usage of its personally identifiable information for canvassing, inclusively commercial, charitable or political goals, without a legal justification.

Section 12: The subject individual of Personally Identifiable Information processing needs to be informed by the responsible of the processing or its representative:

- a. Of the identities of either the responsible of the processing or its representative.
- b. Of the objective/goal that the processing aims at.
- c. Of the clear definition of the mandatory and optional information that are asked and the answers provided/ given;
- d. Of the recipients or categories/sorts of recipients of the information;
- e. Of the mode of application of his opposition, accessibility and amendment rights.

Section 13: Any individual who declines his identity has the right to interrogate the offices or entities encharged of the implementation of the digital processings; which list is accessible to the public in order to know if the



processings are based on nominal information and, if need be/necessary, can be given discovery of it.

Section 14: The incumbent of accessibility right can be given discovery of his information. The communication, in clear language, must be consistent to the records.

A copy is delivered to the incumbent of accessibility right that he in fact demands on payment of a lum sum which amount varies according to the category of the processing, and is fixed on decision of the Commission and confirmed and signed by the Minister of Finance.

However, after consultation of both parties, upon reference by the responsible of the file, the Commission may allowed him:

- Reply deadlines
- Authorization to disregard a number of demands that appear manifestly excessive for their number, repetitive or systematic.

In case of risk of dissimulation or missing of information mentioned in the first line of the presente section, and even before the practice of any jurisdictional claim, the competent judge may be seized to ordain all measures to avoid that dissimulation or missing.

Section 15: Any individual who declines his identity, may request from the responsible of a processing that, depending of the cases, his erroneous, incomplete, equivocal, expired personally identifiable information; or of which the collecting, the usage, the communication or the storage are forbidden; be rectified, completed, updated, secured or deleted.

When the concerned individual makes the demand, the offic e or the entity involved must deliver a free copy of the modified recording.

In case of contestation, the responsibility of evidence lies to the qualified office to deal with the accessibility right, only if it is established that the contested information were communicated by the concerned individual or with his consent.

When the incumbent of the accessibility right brings a modification to the recording, the payment made based on the provisions of the Section 14 is reimbursed.

Section 16: Upon approval of the Commission, a registered file may be completed or even automatically corrected/rectified when the entity that hold custody of it notices the inaccuracy or the incompleteness of a registered information contained in a file.

If any information is passed on to a third party, its rectification or its deleting/cancelling should be notified to such third party, except if exemption is awarded by the Commission.

Section 17: As regard to the processings related to the Homeland Security, the defence and the Public Safety, the demand is sent to the Commission, which delegate on of its members, that belongs or once belonged to the Supreme Court or to the Chamber of Accounts, to carry out all the investigations possible and to make the needed modifications. This delegated member can be assisted by another member of the Commission.

The applicant is notified that verifications have been made.

Section 18: When the exercice of the accessibility righth applies to forensic/medical related information, these ones may only be disclosed to the subject individual by a medical officer/Doctor/Phisician that he elects for this purpose.

#### **CHAPTER IV**

##### **COMMISSION IN CHARGED OF THE PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION AND PROCESSINGS VERIFICATION/CONTROL**

Section 19: It is instituted, in the Republic of Benin, an entity that protects the personally identifiable information and the verification/control of their processing, which is entitled “ National Commission of information pravacies ”(NCIP) hereinafter named Commission.

The Commission sees to the application of the provisions of the present law.

Section 20: The Commission is an independent administrative structure.

It discharges a public service mission.

It is endowed with the status, the administrative and managing autonomy.

It does not receive instruction/order from any administrative or political authority.

Section 21: The Commission sees to the implementation of the processing of the personally identifiable information according to the provisions of the present law.

In this regard, it:

- a. Informs and advise all the individuals concerned and the responsible of the processing of their rights and obligations;
- b. Verifies/controls the designing and the carrying out of the processings;
- c. Recieves the complaints, requests and claims related to the carrying out of the processings of the personally identifiable information and informs the makers of what their followings are.
- d. Informs, without delay, the Public Procecuter, according to the provisions of penal procedure code, of the violations and provisions of the present law, constitutive of penal infringements;
- e. Sees to the developepment of the new technologies of information and communication and discloses its appreciation of the consequences and development on the protection of privacy liberties;
- f. Transmits to the authorities, the propositions of legislative or regulatory modifications that he deems susceptible to

improve the protection of individuals against the use of the new technologies of information and communication.

The Commission is involved in the international negotiations having an incidence on the processing of personally identifiable information and cooperates with the authorities in charge of the protection of personally identifiable from other foreign countries.

Section 22: A Government Representative, delegated by the President of the Republic, sits by the Commission.

He can, ten(10) days after a deliberation, provoke a second or another deliberation.

Section23: The Commission is composed of eleven(11) members as it follows:

- Three (03) Members of the Parliament delegated/apointed by the National Assembly and based on the political configuration;
- One (01) Member of the Economic and Social Council elected by his peers;
- Two (02) qualified individuals with computer Science literacy, a Master Degree and at least ten (10) years of experience, selected by the National Assembly and based on the political configuration;
- One (01) personality selected/appointed in the Government Council Session by the President of the Republic;
- Two (02) judges from the Supreme Court with at least fifteen (15) years of experience, elected by his peers:
- One (01) member of the Chamber of Accounts of the Supreme Court with at least fifteen (15) years of experience, elected by his peers;
- One (01) Lawyer with at least (15) years of experience, elected by his peers.

The Commission is led/managed by a board of three(03) members. It elect a President, a Vice-President, and a Secretary from within.

Section 24: The members of the Commission, once selected or elected are appointed by order in council.

Prior to the start of their function, the members take an oath before the Court of Justice of Cotonou in a solemn sitting, the oath says the following:

*“ I solemnly swear to take on/fulfill my function/responsibility of member of the Commission in charge of the protection of personally identifiable information, in full liberty and impartiality in dignity and loyalty and keep the secret of the deliberations”.*

The staff/personnel recruited by the National Commission of Information Privacy and Liberties takes an oath before the magistrates' Court of Cotonou in these terms:

*“ I swear to fulfill well and loyally my responsibilities of agent of the Commission in charge of the personally identifiable information in full liberty and impartiality and to keep the secret of the deliberations”.*

Section 25: The members of the Commission are appointed for a Five(05)-year-term of office renewable once.

Section 26: The mode of governance/functioning of the Commission is fixed by the statutes.

Section 27: The status of member of the Commission is inconsistent with the one of member of the Government.

No member of the Commission may:

- Take part in any deliberation or initiate any verifications related to an entity within which he, has a direct or indirect interest, holds responsibilities or detains any mandate.
- Take part in any deliberation or initiate any verifications related to an entity within which he has, during the thirty-six (36) months preceding the deliberation or the verifications, had a direct or indirect interest, held any responsibilities or detained any mandate.

Section 28: The members of the Commission are irremovable for the term of their mandate.

However, in case of serious duly established mistake/violation committed by any member of the Commission or the deprivation from the title for which he has been elected or selected, his responsibilities are terminated and his replacement made according to the provisions of the law and statutes of the Commission.

The mandate of the successor covers the remaining time to the end of the term. The latter may be appointed for only one mandate.

Section 29: The members and staff of the Commission are called to observe a strict sense of professionalism/confidentiality for the information that are disclosed to them within the scope or by the occasion of their function.

Section 30: The Information Technologies Professionals (IT Pros) solicited, either to inform the Commission, or to witness before it, are as such freed/untied from the need of the discretion of their duty.

Section 31: Indispensable credits are annually allocated to the Commission for its smooth running. These credits are quoted/inscribed in the Government's Budget.

The Commission may receive subventions from international organizations that the Government is member of and from any other entities legally constituted. It may also benefit resources from the running of its own businesses.

Section 32: The Commission receives notifications of creation of digital processings and gives its approbation in the cases specified/provided by the present law.

Section 33: The Commission informs the public of/provides the public with the list of the authorized processings.

Section 34: The Commission receives and instructs the complaints according to its mission.

Section 35: The Commission may ask the presiding judges of the courts of appeal or the presidents of administrative jurisdictions to delegate a judge from within their competence, eventually assisted by experts, for the missions of investigation and verification carried out under their direction/leadership.

Section 36: In order to fulfill its missions/responsibilities as assigned by the law, the Commission has the legal capacity to authorize a few processings, to adapt measure of simplification or of exemption of declaration and to define the modalities of human rights, particularly in information matter.

Section 37: The Commission may charge the responsables of the files to provide it with all necessary information on the digital files that they use.

Section 38: The Commission uses all mediums it deems appropriate to inform, the government/public authorities, the private organizations and the representatives of non governmental organizations, of the decisions, and advices it pronounces in matter of protection of privacies.

Section 39: The Ministers, government/public authorities, managers of public or private entreprises, leaders of divers groups and generally the detentors and users of processings or files of personally identifiable information may not oppose to any action of the Commission. They can take all necessary measures in order to facilitate its mission.

Section 40: The decisions of the Commission that interfere with citizen's interests are susceptibles of appeal before the competent administrative jurisdiction.

Section 41: the digital processings carried out by public or private entities and contain personally identifiable information should, prior to their implementation, be declared with the Commission or be inscribed/reported in

a log book held by the individual that the responsible of the processing assigned to.

Section 42: Are not subjects to any obligation of declaration:

- a) The processings of personally identifiable information carried out by public or private entities for their general book keeping/accountancy;
- b) The processings of personally identifiable information carried out by public or private entities and are related to the management of the salaries of their employees;
- c) The processings of personally identifiable information carried out by public or private entities for the management of their suppliers;
- d) The processiing of personally identifiable information carried out by associations and non profit entities exclusively based on their corresponding strategic goals/objectives information and involving their members and the different stakeholders ( individuals with whom they develop/keep regular contacts) within the scope/frame of their activities.

Section 43: The processings indicated below may only be carried out upon the authorization and prior control of the Commission because of the particular risks for the rights and privacies or when the content and their motives are susceptible to interfere with the privacy of the individuaal involved in the processing of personally identifiable information:

- a) The Processings that include a national identification number as well as all nationwide processings taking census of the entire population or part of it;
- b) The processings that include sufficient biometric data/information for the tracking of individuals' identities;



- c) The processings that include health related information/data of individuals or their situation/location;
- d) The processings that include information/data related to the infrengements and condemnations;
- e) The processings related the homeland security, the defence or the public safety and the ones that deal with the prevention, researching, the verification or the tracking of penal infrengements or the execution of penal condemnations;
- f) The processings that aim at the interconnexion of files corresponding to different interests;
- g) Processings that can deny individuals the favour/benefit of a right, a performance or a contract;
- h) Processings that allow for transfers of personal data/information to other foreign countries when the processing warrants sufficient degree of privacy protection as well as liberties and unalienable human rights, also for contractual terms or internal rules that it is subject to.

Section 44: When the Commission is seized, as provided in the Section 43 of the present law, it must adjudicate within a two (02) months allotted time starting from the date of reception of the demand for authorization, unless in the cases provided in the Section 17.

The demand made with the Commission, that the latter does not adjudicate until the expiring of the allotted time provided in the preceding indented is considered favourable.

Section 45: The declaration must contain:

- a. The identity and the address of the officer in charge of the processing of personally identifiable information/data;
- b. The objective(s) of the processing;

- c. The recorded/stored personally identifiable information/data, their origin and the duration of their conservation/keeping;
- d. The individuals able to be granted discovery of/given access of the information/data or individuals to whom they can be passed on to.
- e. The offices where the individuals involved can exercise their accessibility rights;
- f. The transfers of personally identifiable information/data for other foreign countries if need be;
- g. The security measures;
- h. The commitment that the processings are made according to the provisions of the present law.

Section 46: The clauses and the content of the declaration quoted in the Section 32 of the present law are stated by the Commission.

## **CHAPTER V**

### **OBLIGATIONS OF THE PROCESING OFFICERS**

Section 47: The members of the Commission as well as the staff of its offices are responsible of the verification/control of the carrying out of the processing. Therefore, they have access, within the frame of their function, to the site/physical plants, facilities, enclosures, equipment or installations which serve for the carrying out of the processing of personally identifiable information/data.

If the either responsible of the site or the responsible of the processing opposes any visit, such visit may be allowed/made upon authorization of the President of the competent Court of first instance or the judge he delegated.

At the end of the visit, a contradictory report of inspections and visits is prepared.

The report is submitted, for observations, to the Commission.

Section 48: All responsible of the processing or his representative must clearly and completely inform all user of the digital communication network:

Of the motive of all action tending to accessing/reaching, electronically, information stored in his connexion end equipment, or to entering, using the same technic, information in his connexion end equipment.

The means he can use to express his opposition.

These provisions do not apply to accessing the information/data stored in the user's end equipment or entering information/data into the user's end equipment:

Be it, for an exclusive motive of allowing or facilitating the digital/electronic communication;

Be it, it is strictly necessary for the supplying of an online communication service when expressly requested by the user.

When personally identifiable information/data have not been collected from the subject individual himself, the responsible of the processing or his representative must provide to the latter the information/data listed in the Section 14 of the presente law, as early as the recording/storing of the information/data or, if a communication of the information/data to other individuals is envisaged later while communicating the first information/data.

When personally identifiable information have initially been collected for another objective/motive, the provisions of the preceding first paragraph lines do not apply to the necessary processings for information/data conservation/keeping for historical, statistical or scientific use. Neither do

Such provisions apply when the subject individual is already aware or his information turns out impossible or requires disproportionate efforts/sacrifices with consideration to the profitability/opportunity of the operation.

Section 49: Unless clear consent of the subject individual, the personally identifiable information/data collected by electronic/digital certification service providers for certificates issuing and conservation needs related to electronic signatures must be directly collected from the subject individual and must only be processed for the motives/objectives for which they have been collected.

Section 50: The responsible of the processing must take all necessary precautions with regard to the nature of the information/data and the risks linked to the processing to preserve the security of the information/data and, inclusively/also prevent their distortion, alteration or that unauthorized individuals have access to them.

Section 51: Personally identifiable information/data processing may be operated by a subcontractor, an individual acting under the subordination of the responsible/officer in charge of the processing or the subcontractor, only if the responsible/officer in charge of the processing gives such instruction.

Any individual processing personally identifiable information/data on the behalf of the responsible/officer in charge of the processing is considered a subcontractor in the view/ of/according to the present law.

The subcontractor must give sufficient warranties to ensure the implementation of the security and confidentiality measures mentioned in the ending lines of the present Section. This requirement does not exempt the responsible/officer of the processing from his obligation to see over the respect of these measures.

The contract between the sub-contractor and the responsible of the processing specifies the obligations that the sub-contractor is subject to in matter of protection of the security and confidentiality of data and specifies that the sub-contractor may take action only when the responsible instructs him.

Section 52: The responsible of the processing of personally identifiable information must immediately report all modifications of the information released to the Commission, including the deletion of the procession.

Section 53: Personally identifiable information may not be stored for a duration longer than the one provided in the Section 5 before being processed for historical, statistical or scientific uses. The processings that are to be secured as long term archives are exempt from the pre-processing formalities provided in the presen law.

A processing carried out with objectives different from the one stated in the first lines of this Section:

- Be it, with full consent of the subject individual;
- Be it, with the authorization of the National Commission of Information Privacies.

## **CHAPTER VI CONDITIONS OF SANCTIONS AND FINAL PROVISIONS**

### **ARTICLE I ADMINISTRATIVE SANCTIONS**

Section 54: The Commission may send a formal notice to a responsible of the processing that does not respect the obligations deriving from this law.

It may also summons the responsible of the processing to stop the breach/ violation noticed in a fixed delay not to exceed eight days(08).

Section 55: When the responsible of the processing does not comply with the formal notice, the Commission may pronounce against him, inconsisent to the following sanctions:

- A pecuniary sanction, excepting the cases where the processings are carried out by the Government;

- An order to cease the processing of the personally identifiable information;
- The cancelling/withdrawal of the authorization issued enforcing the present law;
- The locking of some personally identifiable information.

Section 56: All sanction pronounced by the Commission may be accompanied with an order to operate, in a delay not to exceed eighth (08) days, any useful modification or suppression/cancelling in the functioning of personally identifiable information processings, subject to the sanction.

Section 57: The sanctions provided by the present law are pronounced in a report made by the Commission. This report is submitted to the responsible of the processing, that may make written or oral observations, and attend or be represented in sessions which end with decisions taking by the Commission. The decisions reached by the Commission are justified and notice is given to the responsible of the processing.

Section 58: The decisions pronouncing/stating a sanction may be subject of appeal before the competent administrative jurisdiction.

Section 59: The amount of the pecuniary sanction is proportional to the importance of the violation/breach committed and to the advantages deriving from such breaches/violations.

Section 60: The following actions are considered important/serious violations:

- Disloyal gathering of personal data;
- Releasing to an unauthorized third party individual personal data;
- Gathering sensitive/classified data, data related to infringements or to a national identification number without observing the legal conditions.

- Gathering or using personal data having as result/consequence to provoke a serious violation of unalienable human rights or to the intimacy of the privacy of the subject individual;
- Preventing the offices of the Commission from executing/operating their verification duty on site or appearing/standing as an obstruction while such duty is being carried out.

Section 61: The Commission may make public/publish the sanctions.

## **ARTICLE II CIVIL SANCTIONS**

Section 62: In case of serious violations or proximate to the rights and privacies mentioned in the Section 2 of the present law, the Commission or the individual whose rights and privacies have been violated, may request through a summary procedure, to the competent jurisdiction, to order if necessary, under obligation, all necessary measure to safeguard these rights and privacies.

Section 63: The victims may seize the competent jurisdiction for indemnification.

## **ARTICLE III PENAL SANCTIONS**

Section 64: Are considered infringements/violations to the present law, without prejudice to the ones provided by the penal code in data processing matter:

- a. Impeding the commission's action:
  - By opposing the execution of the missions assigned to its members or to the entitled agents/Privacy Practitioners;
  - By refusing to provide the Commission Members or the entitled agents/Privacy Practitioners with useful information and documents

for their mission, or dissimulating such documents and information, or by removing them;

- By providing false/erroneous information different from the ones contained in the records when the request is made or records that do not present their contents directly accessible;
- b. Operating the processings of personal data, even by negligence, without respecting the pre-required formalities for their carrying out as provided by the present law;
- c. Excepting the cases where the data processing was made according to the provisions of the present law, operating or ordering a processing of personal data containing sensitive data relating to infrengments/violations or relating to national identification number;
- d. Operating or ordering a processing of personal data without carrying out the measures prescribed by the provisions of the present law;
- e. Collecting/gathering personal data by fraudulent, disloyal or illicit means;
- f. Diverting and/or manipulating information by any privacy practitioner holder of personal data at the occasion of their recording, their classification, their transmission or any other kind of processing;
- g. Operating the processing of personal data distinguishing an individual though the request for rectification or opposition from the subject individual is based on legitimate motives;
- h. Violation of the present law in the provisions related to personal information;
- i. Violation of the present law in the provisions related to accessibility rights;



- j. Over-keeping personal data for a period of time longer than the normal provided prior to declaration to the Commission only if such conservation is made for historical, statistical or scientific reasons in the conditions as defined by the present law;
- k. Any privacy practitioner having collected/gathered, at the occasion of their recording, classification, transmission or any other kind of processing , of personally identifiable data/information which disclosure will result in, a denigration of the individual, or to the intimacy of his privacy, to share without the subject individual's authorization/consent, such information/data with a third party who is not qualify to receive them;
- l. Implication in any association or any established combine in order to commit one or several infrengments provided by the present law.

Section 65: The infrengments mentioned in the Section 64 of the present law are punished by a five (05) to ten (10) years prison sentence plus a Ten Millions (FrCs CFA 10, 000,000.00) to Fifty Millions (FrCs CFA 50, 000, 000.00) fine or only one of these two penalties.

Aiding and abetting are also punished by the same penalties.

The Tribunal may order the suppression of all or part of the personally identifiable information/data which processing resulted in the infrengment.

Section 66: The present law which abrogates any previous contrary provisions, will be as Government Act/law.

***Cotonou, May 22, 2009***

By The President of the Republic, Head of State, Head of the  
Government,

Signature

Dr. Boni YAYI

The Minister of Homeland, and Public Safety,

Signature

**Armand ZINZINDOHOUE**

The Minister of Justice, Legislation and Human Rights,  
Spokesperson of the Government,

Signature

**Victor Prudent TOPANOU**