Law No. 2013-015 of May 21, 2013

Protection of personal data in the Republic of Mali

The National Assembly deliberated and adopted at its session of May 9, 2013;

The President of the Republic promulgates the law, the content of which is as follows:

Chapter 1: Of the object

Article 1 : By this law, the State of Mali ensures to any person, natural or legal, public or private, the protection of their personal data, without distinction of race, origin, color, sex, age, language, religion, fortune, birth, opinion, nationality or other.

The law ensures that any processing, in whatever form, respects the fundamental rights and freedoms of natural persons. It also takes into account the prerogatives of the State, the rights of local authorities, the interests of businesses and civil society.

Article 2: Information technology must be at the service of every person. It must respect human identity , human rights, privacy, public and individual freedoms.

Everyone has the right to the protection of personal data concerning them.

No decision having legal effects on a person may be taken on the sole basis of a treatment computer science intended to define *the* profile of the person concerned or to evaluate certain aspects of their personality.

Chapter 2 : Definitions

Article 3: For the purposes of this law, we understand:

about:

1°/ Electronic communication: emission, transmission or reception of signs, signals, writings, images or sounds, by electronic or magnetic means.

2°/ Temporary copy: copied data temporarily in a dedicated space, for a limited period of time, for the operating needs of the processing software.

3°/ Consent of the person concerned:
any expression of express, unequivocal, free, specific and informed will by which the person concerned or his legal, judicial or conventional representative, accepts that his personal data be processed.

4°/ Recipient of personal data processing:

- any person authorized to receive communication of these data other than the person concerned, the data controller, the processor and the persons who, by reason of their functions, are responsible for processing the data;

the authorities legally entitled to request the data controller to communicate personal data to them, in the context of a specific mission or the exercise of a right of

communication.

5°/ Personal data : personal data or personal data is information existing in various forms and indirectly to identify directly or allowing a person, by reference to a registration number or to one or more elements specific to their physical, physiological, biometric, genetic, psychological, cultural, social or economic identity. They can be universal identifiers allowing several files constituting databases, or to carry out their interconnection.

6°/ Civil status data: in addition to identifying a natural person, it serves to prove that they belong to a family.

7°/ Genetic data: any data concerning the hereditary characteristics of an individual or a group of related individuals.

8°/ Personal data: this corresponds to the surnames, first names, physical or electronic address of a person, their social security references,

his payment card or bank account number, vehicle registration plate, identity photo, fingerprint or

DNA.

9°/ Heritage data: it is made up of a set of inter-related data in the form

of standardized notices allowing the presentation in a uniform and controlled manner of the essential information on the works collected, during inventory, census, study or protection operations.

10°/ Professional data: this concerns, among other things, first names and surnames, addresses, telephone and fax numbers, localities and places

of service, as well as responses to individual or collective information forms.

11°/ Sensitive data: any personal data relating to religious, philosophical, political, trade union opinions or activities, sexual or racial life, health, social measures, prosecutions, criminal or administrative sanctions.

12°/ Health data: any information concerning the physical and mental state of a person concerned, including their genetic or biological data.

13°/ Personal data file:
any structured set of accessible data

according to specific criteria, whether this set is centralized, decentralized or distributed in a
functional or geographical.

14°/ Interconnection of personal data: any connection mechanism consisting of the linking of data

processed for a specific purpose with other
data processed for identical or different or related purposes by one or more data controllers
treatment.

15°/ Third country: any State other than Mali.

16°/ Data subject: any person who is the subject of personal data processing .

17°/ Direct prospecting: any solicitation made by sending a message, whatever the medium or nature, in particular commercial, political or charitable, intended to

promote, directly or indirectly, goods, services or the image of a person selling goods or providing services.

18°/ Data controller: any person who, alone or jointly with others, makes the decision to collect and process data at

personal character and determines its purposes.

19°/ Subcontractor: any natural or legal person, public or private, any other body or association which processes data on behalf of the data controller.

The subcontractor(s) may be considered as delegates of the data controller(s) whether or not they are part of a network.

20°/ Remote service : any value -added service provision , based on telecommunications and/or IT, aimed at enabling, interactively and remotely, a natural or legal person, public or private, the possibility of carrying out activities, procedures or formalities.

21°/ Third party: any natural or legal person, public or private, any other body or association other than the person concerned, the data controller, the subcontractor and the

persons who, under the direct authority of the controller or processor, are authorized to process the data.

22°/ Processing of personal data: any operation or set of operations carried out using automated or non-automated processes and applied to data, such as collection, exploitation, recording, organization, storage, adaptation, modification, extraction, backup, copying, consultation, use, communication by transmission, dissemination or any other form of making available, reconciliation or interconnection, as well as the locking, encryption, erasure or destruction of personal data.

Chapter 3 : Scope of application

Article 4: The law applies to all processing of personal data carried out in whole or in part on national territory.

Article 5: The following are subject to this law:

1°/ any processing of **personal data by the State, local authorities, personalized organizations, natural persons and legal persons under private law;**

2°/ any processing implemented by a person responsible, established or not on the national territory, excluding means which are only used for transit purposes on the territory;

3°/ any processing of data concerning public security, national defence, the investigation and prosecution of criminal offences or the security of the State, even if linked to an important economic or financial interest of the State, subject to the exceptions provided for by this law or, where applicable, the specific provisions provided for by other texts.

Article 6: The following are excluded from the scope of this law:

1°/ data processing carried out by a natural person within the exclusive framework of his or her personal or domestic activities, provided however that the data is not intended for systematic communication to third parties or for dissemination;

2°/ temporary copies made as part of technical activities of transmission and provision of access to a digital network, for the purpose of automatic, intermediate and transitory storage of data and for the sole purpose of

allow other recipients of the service the best possible access to information transmitted.

Chapter 4: Principles

Article 7: Personal data must:

- **be collected and processed in a fair, lawful and non-fraudulent manner for specific, explicit and legitimate purposes;**
- **not be used for other purposes;**
- **be adequate, proportionate And relevant to the purposes for which they are collected or used;**
- **be accurate, complete and, if necessary, updated;**
- **be kept in a form which permits identification of the persons concerned for no longer than is necessary for the purposes for which they are collected or used.**

These provisions do not prevent the retention and use of the data processed.
for the purposes of archives management or for historical, statistical or scientific purposes in accordance with the terms defined by law.

Section 1: On the obligation of security

Article 8: The data controller takes all necessary precautions to preserve data security.

In particular, it must prevent them from being distorted, damaged or **accessed by unauthorized third parties .**

The legally authorized authorities within the framework of a specific investigation mission, such as the judicial authority, the judicial or control police, may ask the data controller to communicate personal data to them.

The subcontractor must provide sufficient guarantees to ensure the implementation of security and confidentiality measures. This
requirement does not exempt the controller from its obligation to ensure compliance with these measures.

Section 2: Sensitive data

Article 9: Any processing of sensitive data is prohibited due to the risks of discrimination and infringement of rights and freedoms.
people.

By way of derogation from the preceding paragraph, sensitive data may be subject to processing with appropriate guarantees defined by the Authority responsible for the protection of personal data , if the processing:

- **is necessary or is implemented for the protection of the life of the data subject or of a third party, when the data subject cannot give consent, due to legal incapacity or material impossibility;**

- **is implemented by an association or any other non-profit organization of a religious, philosophical, political or union nature whose sole purpose is the management of their members;**

- **is necessary for the establishment, exercise or defense of a legal right.**

Section 3: Treatment of infringement or conviction

Article 10 : **Processing of personal** data **Personal relatives to infractions And convictions can only be put into effect work by:**

- **courts and public authorities managing a public service acting within the framework of their legal powers;**

- **legal assistants, for the strict need of carrying out the missions entrusted to them by law;**

- **other legal entities, for the strict purpose of managing disputes relating to the offences of which they were victims.**

Section 4: Transfer of personal data abroad

Article 11 : The data controller may transfer personal data to a foreign State:

- when the recipient State ensures a sufficient level of protection of individuals, noted by the Authority responsible for the protection of personal data, due to its internal legislation or commitments made at international level and these measures are effectively applied;

- by decision of the Authority responsible for the protection of personal data, when the transfer and processing by the recipient of personal data guarantees a sufficient level of protection of privacy as well as of fundamental rights and freedoms of persons, in particular because of the contractual clauses or internal rules to which it is subject.

Chapter 5: Individuals' rights regarding data processing

Section 1: Right of access and rectification directs

Article 12: Any person has the right to obtain from the controller:

- **the communication, in a comprehensible form, of all data concerning it as well as any available information as to their origin;**

- **the information and reasoning used in computerized processing whose results are opposed to him.**

The applicant exercises his right of access free of charge on site or remotely . His right of access is granted request without delay.

A copy of the data concerning him, in accordance with the content of the processing, is provided to the interested party. at his request.

In case of risk of concealment or disappearance data, the Authority responsible for the protection of personal data may order any appropriate measure to this effect.

Article 13: Any person providing proof of their identity may require the data controller to, as the case may be, rectify, complete, update , lock or delete **personal data concerning them which are inaccurate, incomplete, ambiguous, outdated, or whose collection, use, communication or storage is is prohibited.**

When the data subject makes a request in writing, regardless of the medium, the data controller must provide proof, free of charge to the applicant, that it has carried out the operations required under the preceding paragraph within thirty (30) days after the registration of the request.

request.

In the event of a dispute, the burden of proof lies with the data controller with whom the right of access is exercised.

When data has been transmitted to a third party, the data controller must take the necessary steps to notify them of the operations.

which he has carried out in accordance with paragraph 1 of this article.

Section: Right of access and rectification indirect

Article 14: When processing concerns state security, defence or public safety, the rights of access and rectification to data are exercised indirectly.

In this case, the request is addressed to the Authority responsible for the protection of personal data, which appoints one of its members to carry out the necessary investigations, with a view to making the necessary modifications.

Where the Authority responsible for the protection of personal data finds , in agreement with the data controller, that the communication of the data contained therein does not jeopardize the security of the State, the defence

or public safety, these data are communicated to the applicant. The applicant is notified, where appropriate, that the following data have been collected: checks.

Section 3: Right to information

Article 15: When personal data are collected directly from a data subject, the data controller must provide the data subject, at the time of collection and regardless of the means and media used, with the following information:

1°/ the identity of the data controller and, where applicable, of his representative;

2°/ the specific purpose(s) of the processing for which the data is intended;

3°/ the categories of data concerned;

4°/ the recipient(s) or categories of recipient(s) to whom the data may be communicated;

5°/ knowing whether the answer to the questions is mandatory or optional as well as the possible consequences of a failure to respond;

6°/ the ability to request to no longer appear on the file;

7°/ the existence of a right of access to the data concerning and rectification of this data;

8°/ the duration of data retention;

9°/ where applicable, transfers of personal data envisaged abroad.

Article 16: Where personal data are not collected from the data subject, the information shall be transmitted to the data subject in accordance with Article

15 of this law.

Article 17: The provisions of Article 15 of this law do not apply:

1°/ to data collected and used during processing carried out by the State or on its behalf and relating to State security, national defence, public safety or the purpose of which is the execution of criminal convictions or security measures, to the extent that such limitation is necessary to comply with the purposes pursued by the processing;

2°/ when the processing is necessary for the prevention, investigation, establishment and prosecution of any offence;

3°/ when the processing is necessary to take into account an important economic or financial interest of the State, including in the monetary, budgetary, customs and tax areas, generally any mission of public interest.

Article 18: Any person using electronic communications networks must be informed clearly and completely by the data controller or his representative:

- the purpose of any action tending to access, by electronic transmission, information stored in its connection terminal equipment, or to enter, by the same means, information in its connection terminal equipment;

- the means at its disposal to achieve this oppose.

These provisions are not applicable in the following cases:

- if access to information stored in

the user's terminal equipment or the recording of information in the user's equipment has the exclusive purpose of enabling or facilitating communication by electronic means;

- or if access is strictly necessary for the provision of a communications service online, at the user's ex-press request.

Section 4: The right to object to being included in processing

Article 19: Any natural or legal person has the right to object, for legitimate reasons, to the processing of personal data concerning them. They have the right, on the one hand, to be informed before these data are , for the first time, communicated to third parties or used on behalf of third parties for prospecting purposes and, expressly informed free of charge, of their right to object to said communication or else part, to be use.

Chapter 6: Personal data protection authority

Section 1: Of the institution, composition, and organization

Article 20 : An authority is established independent administrative body called the **Personal Data Protection Authority , abbreviated as (Apdp).**

Article 21: The Authority includes a collegiate deliberative body composed of fifteen (15) members appointed for a non-renewable term of seven (7) years, as follows:

- Two (2) qualified persons designated by the President of the Republic;
- Two (2) deputies appointed by the National Assembly at the rate of one deputy for the majority and one deputy for the opposition;
- Two (2) National Councilors appointed by the High Council of Local Authorities;
- One (1) qualified person designated by the Minister responsible for civil status;
- One (1) qualified person designated by the Minister responsible for internal security;
- A (l) qualified person designated by the Minister responsible for Information Technology;
- Two (2) magistrates, one (1) from the judicial system and one (1) from the administrative system, appointed by the Supreme Court;
- Two (2) qualified representatives appointed by the National Human Rights Commission the man ;
- One (1) qualified representative designated by the Coordination of associations and NGOs feminine;
- One (1) qualified representative designated by the National Council of Civil Society.

Article 22: Membership of the Personal Data Protection Authority is incompatible with membership of the government or any management position within a public or private structure.

If a member of the Data Protection Authority Personal data is located in one of the incompatibilities provided for in the preceding paragraph, the interested party has a period of thirty (30) days to choose between his former function and that of member of the Authority. Failing this this option, the President of the Authority takes the necessary measures to ensure compliance with these provisions.

Article 23: The terms of appointment of members of the **Personal Data Protection Authority are those set by the status of the structure from which each member comes.**

Article 24: The nominal list of members of The Personal Data Protection Authority is established by decree taken in Council of Ministers on the proposal of the Prime Minister.

Article 25: Members of the Authority protection of personal data are bound by professional secrecy in accordance with the texts in force.

Article 26: The Authority establishes its internal regulations and may delegate certain of its powers to its president.

The matters subject to this delegation must be limited to strict administrative functions and management required by the circumstances and never undermine the essential prerogatives of the Authority.

Article 27: In the context of its missions, the Authority does not receive any injunction or instruction, directly or through its members, from any other authority.

Article 28: It is allocated annually to the Authority resources necessary for its operation.
These resources are included in the State budget.

The Authority may receive grants from of international organizations of which the State is member.

The President of the Authority is the authorising officer of the budget.

A decree taken in council of ministers sets the method of remuneration of members of the Authority, on the proposal of the Prime Minister.

Article 29: The accounts of the Personal Data Protection Authority are subject to controls administrative and jurisdictional provided for by the regulations in force.

The Personal Data Protection Authority shall file its annual accounts for the previous financial year no later than 31 March of each year with the accounts section of the Supreme Court and, where applicable, the court which replaces it.

Article 30: The **Personal Data Protection Authority is headed by an office of five (5) members, elected from among its members, including a President.**

The President is assisted by two (2) Vice-Presidents and two (2) Rapporteurs,

The President, the Vice-Presidents and the Rapporteurs are elected under the same conditions, by two-round majority vote of the members of the Authority,

If the absolute majority is not acquired in the first round, a simple majority is sufficient in the second round of voting,

The vote is personal and secret. However, in all matters, a member of the authority who is absent or prevented from acting may give a colleague a duly legalized proxy,

Proxies given by members of the Personal Data Protection Authority are subject to the general regime of proxies. No member of the authority may hold more than one proxy.

Section 2: Missions

Article 31: The **Personal Data Protection Authority is responsible for ensuring the protection of personal data and participating in the regulation of the sector.**

In this capacity, she is responsible for:

- **set the standards and purposes of the collection, processing or storage of data personal**
- **give prior authorization in the form of approval for any data interconnection;**
- **allow data transfer;**
- **inform and advise data subjects and data controllers of their rights and obligations;**
- **ensure that the processing cannot pose any threats to data relating to private life;**
- **receive complaints relating to the implementation implementation of data processing at personal character;**
- **carry out the necessary checks on the regular processing of personal data;**
- **impose administrative sanctions on any data controller in the event of failure to comply with its obligations;**
- **immediately notify the competent Public Prosecutor of any offences of which it is aware concerning the fraudulent handling of personal data;**
- keep the directory of **personal data processing available to the public;**

- give its opinion on any draft law or decree relating to the protection of personal data;

- ask the government to make any necessary changes to the texts, or to adopt, where appropriate, any new text necessary for the sound protection of personal data.

Article 32: The Personal Data Protection Authority is involved in the preparation and definition of the Malian position in any international negotiation concerning the field of personal data protection. It participates in Malian representation in international and community organizations competent in this field.

Article 33: The Authority receives declarations of creation of computer processing operations, authorizes them or gives its opinion in the cases provided for by this law and keeps available to the public the list of processing operations which have been the subject of a declaration or of an authorization.

Article 34: The Authority receives and investigates complaints relating to its mission.

It informs, by any means it deems appropriate, public authorities, private bodies and representatives of civil society of the decisions and opinions it gives with regard to the protection of freedoms.

It may decide on information or on-site monitoring missions.

Article 35: The Authority decides on the most appropriate publicity measures with regard to the authorization decisions, recommendations, exemption standards, sanctions and denunciations that it adopts.

Article 36: The Authority shall draw up an annual activity report which it shall submit to the Prime Minister no later than the end of the first quarter of each year. This report shall be published in the Official Journal.

Article 37: Ministers, public authorities, managers of public or private establishments or companies, heads of various groups and more generally holders or users of personal data processing or files cannot oppose the action of the Authority and must take all useful measures to facilitate its stain.

Article 38: No member of the Personal Data Protection Authority may be prosecuted, investigated or judged for opinions expressed by him during the meetings of the Authority.

The members of the Personal Data Protection Authority are entitled, in accordance with the rules set out by the penal code and special laws, to protection against threats, insults, insults or defamation which they may be subjected to.

be the object in the exercise of their function. They are entitled to compensation, where appropriate, for any damages they suffer in this regard.

Section 3: Operating procedures of the Personal Data Protection Authority

Article 39: The Personal Data Protection Authority meets as of right, in ordinary session, two (2) times per year.

However, it may meet in session extraordinary at the request of its President or of half of its members.

The sessions are not public.

Article 40: Sessions are convened by the President of the Authority, who ensures the policing of the sessions.

However, the inaugural session is convened by the Prime Minister and chaired by the oldest member, until the election of the President of the Authority.

Article 41: The duration of ordinary sessions does not **may exceed ten (10) days.**

Article 42: Duration of extraordinary sessions cannot exceed five (5) days.

Article 43: Sessions are convened for a specific and limited agenda. They are prepared by the President of the Authority, who has a Secretariat for this purpose. This Secretariat is that of the Personal Data Protection Authority .

Article 44: Decisions of the Authority Protection of Personal Data are recorded by deliberations or minutes.

However, regulatory decisions

of the college are noted only by deliberation of the Authority which has all the prerogatives of public power recognized to the administration.

Article 45: The President of the Authority represents the Authority in civil life and in court. He has regulatory power. In this capacity, he makes decisions and other categories of regulatory acts.

Article 46: The President of the Authority issues to the users a receipt noting any request or complaint made and submitted to the Authority.

This receipt mentions the subject of the request or complaint and the user's commitments.

Article 47: The Personal Data Protection Authority takes its decisions by a majority of 2/3 of its members.

Article 48: The acts of the Authority are acts administrative matters subject to administrative and legal appeal.

The appeal is exercised at the level of the President of the Authority.

Article 49: The Personal Data Protection Authority adopts its internal regulations at its inaugural session.

Article 50: Members of the Authority protection of personal data receive session allowances and travel allowances in the performance of their mission.

of

Article 51: A deliberation of the Authority of protection of personal data sets, within the limits of the financial means made available to it, the daily amount of the compensation provided for in the preceding Article 50. This amount takes into account the scales usually applied at the level of similar Institutions.

Article 52: The State provides the Personal Data Protection Authority with the material and human resources necessary to carry out its mission.

Chapter 7: Reports of the Personal Data Protection Authority with data controllers and ordinary users

Article 53: The Data Protection Authority personal character ensures the coordination and control of the processing of personal data throughout the national territory.

Article 54: Religious denominations, political parties or trade unions may keep a register of their members or their correspondents in the form of computerized data which is beyond the control of the Personal Data Protection Authority.

Article 55: Processing of personal data jurisdictions, public authorities acting in within the framework of their legal attributions, personalized public bodies, communities territorial entities are not automatically subject to the obligation to declare their operations. data processing under their status.

Data controllers acting on behalf of personalized public bodies and local authorities are only subject to the obligation to declare their processing operations on condition that an agreement is signed between the Personal Data Protection Authority and the Authorities responsible for said bodies.

However, the Authority has all means of control over data held at their level with regard to personalized organizations and local authorities .

Chapter 8: Sanctions

Article 56: Without prejudice to the powers of other prosecuting authorities in matters of offence, the President of the Personal Data Protection Authority reports to the Public Prosecutor any user in violation of the law in the area of personal data .

personnel, or files a complaint against the person concerned before the competent courts, for the application of the criminal sanctions provided for by the legislation in force.

Article 57: Data processing managers declare to the Protection Authority the operations they intend to carry out for a given purpose.

If this formality has been omitted in bad faith, the Protection Authority shall impose on the person responsible for

processing of data in question the sanction appropriate administrative measure that it considers, depending on the seriousness of the fault.

Article 58: Unless otherwise provided for by this law in matters of information technology, the classification of offences and the penalties applicable to them are those defined by the Penal Code, the Code of Persons and the Family, the electoral law and other laws which establish offences in the area of the protection of personal data .

The procedure followed for the repression of offences is that set out in the Code of Criminal Procedure.

Article 59: Without prejudice to criminal sanctions, the Personal Data Protection Authority imposes administrative and financial sanctions arising from the application of this law and may institute, by legally made regulations, simple police fines.

Article 60: Civil action is subject to the conditions set by the Code of Civil, Commercial and Social Procedure and the General System of Obligations in the Republic of Mali.

Article 61: Administrative sanctions established by this law are:

- the warning against all data controller acting in good faith who has not complied with the administrative formalities for the collection, processing and management of data provided for by this law or by the regulatory acts of the Personal Data Protection Authority;

- formal notice to the offending data controller, with the aim of requiring them to comply with the texts;

- the injunction to cease personal data processing activities against any data controller, in the event of misconduct;

- the withdrawal of approval from any person responsible for data processing if necessary noted by the Protection Authority.

Article 62: In the cases provided for in Article 61 above, the Personal Data Protection Authority may use all technical means in its possession to ensure the automatic execution of its decision.

Article 63: Sanction decisions administrative decisions are justified, failing which they are null and void, and notified to the interested parties.

Article 64: In addition to criminal penalties involving deprivation of liberty, financial penalties may be imposed on any offender, in accordance with the provisions of Articles 65, 66 and 67 below of this law.

Article 65: Are punishable by a fine of five million (5,000,000) to twenty million (20,000,000) of francs:

1°/ the act of communicating to third parties not authorized or to access without authorization or unlawfully to personal data involving cause fundamental rights and freedoms individual or private life;

2°/ the diversion of purpose or any change of purpose of a collection or a processing of personal data, without express and reasoned authorization from the Personal Data Protection Authority;

3°/ collecting data by fraudulent, unfair or illicit means or carrying out a nominative processing of information concerning a natural person despite their opposition, when this opposition is based on legitimate reasons relating to their fundamental rights or their private life;

4°/ the automated processing of personal data for the purpose of research in the field of health, in violation of laws and regulations;

5°/ the act, except in cases provided for by law, of placing or storing in computerized memory personal data relating to offences, convictions or security measures national.

This offence applies to non-automated or machine-generated files whose use does not fall exclusively within the exercise of the right to privacy;

6°/ the act, by any person, of collecting, on the occasion of recording, classification, transmission or another form of

processing of personal information, the disclosure of which has the effect of harming the honour and reputation of the person concerned or

the privacy of his private life, to bring said information **to the attention of the person concerned without his permission.**

knowledge of a third party who does not have the capacity to receive them;

7°/ hindering the action of the Personal Data Protection Authority:

- **either by opposing on-site checks;**
- **either by refusing to communicate to its members or agents the information and documents useful for the mission entrusted to them, or by concealing or making said documents disappear.**

Article 66: The following shall be punished by a fine of two million five hundred thousand (2,500,000) to ten million (10,000,000) francs:

1°/ the act of carrying out or having carried out a automated processing of personal information

without taking all precautions to preserve the security of said information, in particular in

preventing them from being deformed or damaged;

2°/ the act of placing or storing in computer **memory , without the prior consent of the person concerned, personal data which, directly or indirectly, reveal racial, ethnic origins, political, philosophical, religious opinions or trade union membership.**

Article 67: In all cases of sanction

financial, the Personal Data Protection Authority may enter into a transaction with the offender, at the latter's request, provided that the scales set by law are respected.

Chapter 9: Transitional provisions

Article 68: Public services and natural or legal persons whose activity consisted, before the date of promulgation of this law , in carrying out, as a principal or accessory activity, processing of personal data have a maximum period of six (6) months,

to comply with the provisions of this Act.

In the absence of this regularization within the aforementioned period, their activities are deemed to be contrary to the provisions of this law and they must cease said activities without delay, failing which, the offenders will be exposed to the sanctions provided for by law.

Chapter 10: Final Provisions

Article 69: The practical provisions for the implementation of personal data not provided for by this law will be supplemented by deliberation of the Personal Data Protection Authority , in accordance with the spirit of the law.

Bamako, May 21, 2013

The Acting President of the Republic,
Professor Dioncounda Traoré