REPUBLIC OF CAMEROON

PEACE – WORK – FATHERLAND

LAW N$_o$ 2024/017 **OF** 23 DEC 2024

RELATING TO PERSONAL DATA PROTECTION IN CAMEROON

The Parliament deliberated and adopted, the President of the Republic hereby enacts the law set out below:

PART I
GENERAL PROVISIONS

CHAPTER I
PURPOSE AND SCOPE

SECTION 1: This law relates to personal data protection in Cameroon. As such, it seeks to guarantee the fundamental rights and freedoms of individuals with regard to the processing of their personal data, regardless of data type, processing method or persons responsible.

SECTION 2: The following shall be covered by the provisions of this law:

- processing of personal data by the State, regional and local authorities or any other natural or legal person;
- processing of personal data relating to any person established or residing in, or transiting through Cameroon;
- processing of personal data by a controller or processor established in Cameroon;
- processing of personal data on a territory where Cameroonian law is applicable under international law or duly ratified international conventions.

SECTION 3: The provisions of this law shall not apply to:

- processing of personal data by a natural person exclusively for the purposes of his/her personal or domestic activities, provided that such data are not intended for systematic communication to a third party or dissemination;
- temporary copies made as part of the technical activities of transmission and access provisioning via a communication network for intermediate and transitory data storage purposes in order to secure, for the other service recipients, optimum access to the information transmitted;
- the processing of personal data solely for literary or artistic purposes, for archival purposes in the public interest, for scientific or historical research, for statistical purposes or for journalistic purposes, regardless of the medium used, in compliance with the rules of professional ethics, in particular the security measures guaranteeing the confidentiality of journalistic sources and the moderation rules applicable to discussion forums set up by publishers of journalistic information.

SECTION 4: The processing of personal data by the competent security and defence authorities shall be governed by separate instruments.

CHAPTER II
DEFINITIONS

SECTION 5: For the purposes of this law and its implementing instruments, the following definitions shall apply:

Anonymization: process of modifying or deleting identifiable personal information from a set of data in order to render such data unattributable to specific individuals.

Authority: independent public body responsible for personal data protection.

Certification: compliance tool designed to meet the needs of professionals seeking to communicate on the data protection level offered by their products, services, processes or data systems measured against the benchmark criteria preapproved by the Personal Data Protection Authority.

Encryption: any technique consisting in transforming digital data into an unintelligible format using cryptological means.

Systematic communication: organized and structured process of transmitting information in a consistent and effective manner, usually in a professional or institutional setting.

Consent: any explicit, unambiguous, voluntary, free and informed expression of will, based on clear, precise and comprehensive information, whereby the data subject or his/her legal representative agrees to the processing of his/her personal data.

Temporary copies: any data temporarily copied to a dedicated space for a limited period of time or for the operational requirements of the processing software.

Standard contractual clauses: clauses in standard contracts drawn up and published by the Personal Data Protection Authority in order to provide a legal framework for the transfer of personal data between parties located in Cameroon and an actor located outside Cameroon, the content of which may be modified only for increasing the protection of the personal data transferred.

Recipient: any natural or legal person authorized to receive personal data.

Recipient of processed personal data: natural or legal person, public authority or any other body authorized to receive data, whether or not a third party.

Data: representation of events, information or concepts in a form that can be processed by a terminal or a programme.

Sensitive data: information relating in particular to religious, philosophical, political or trade union opinions and activities, banking transactions, racial or ethnic, linguistic or regional origin, sex life, genetics, biometrics, health, legal proceedings, and criminal sanctions.

Personal data: information relating to an individual making it possible to identify him/her directly or indirectly, in particular by reference to any identification number or to one or more factors specific to his or her physical, psychological, genetic, mental, cultural, socio-professional or economic identity, in particular a name, a photograph, a fingerprint, a postal address, an e-mail address, a telephone number, a social security number, an internal personnel number, a digital identifier, an Internet Protocol address, a computer connection identifier or a voice recording.

Data protection impact assessment: procedure for analysing the likelihood and severity of risks to individual rights and freedoms as a result of the processing of personal data.

File: set of structured personal data that can be accessed on the basis of specific criteria, whether such set is centralized, decentralized or distributed functionally or geographically.

Interconnection of files: connection mechanism consisting in linking personal data processed for a specific purpose with other data processed for the same or different purposes or linked by one or more controllers.

Direct provision of information society services: any service normally provided for remuneration or, where appropriate, free of charge, at a distance, by electronic means and at the individual request of the service recipient.

Data subject: any person whose personal data are processed.

Data portability: possibility for an individual to retrieve some of his/her personal data in an open and machine-readable format and to store it in a personal space or to transfer it to another controller for further use.

Profiling: automated processing of personal data consisting in using it to assess some personal aspects of an individual, in particular his/her health, preferences, location and economic situation.

Direct prospecting: solicitation of a data subject, regardless of medium or type, in particular for commercial, political or charitable purposes, to promote, directly or indirectly, goods, services or the image of a person.

Pseudonymization: technique used to replace directly identifiable data with artificial identifiers in order to protect individual privacy.

Data controller: natural or legal person who, solely or with others, collects and processes personal data and determines the means and purposes of such collection and processing.

Technical specifications: explicit set of technical requirements, criteria or constraints that a data processing service must meet.

Information society: society in which access to and the transmission of information play a vital role in economic, social and political activities. Such a society is characterized in particular by the use of information and communication technologies (ICT) such as the Internet, social media, computers, mobile phones and geographic information systems.

Sub-processor: any natural or legal person that processes personal data on behalf of and under the direction of the controller.

Information system: set of resources and devices, whether interconnected or isolated, used to process information necessary for the functioning of an organization.

Processing: operation or set of operations performed on personal data, whether or not by automated or semi-automated means, in particular the collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, blocking, erasure or destruction.

International data transfer: transfer of personal data beyond the borders of one country to another, whether to a third country or to an international organization.

Personal data breach: any breach of the security of personal data resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to such data transmitted, stored or otherwise processed.

PART II
LEGAL REGIME OF THE PROCESSING OF PERSONAL DATA

CHAPTER I
PERSONAL DATA PROCESSING PRINCIPLES

SECTION 6: The processing of personal data shall respect individual privacy.

SECTION 7: Whoever processes personal data shall ensure its confidentiality on digital communication networks or any other medium.

SECTION 8: Every person shall ensure the legality and integrity of the content of personal data transmitted through his/her network, in particular when such content is prejudicial to human dignity, honour and privacy.

SECTION 9: (1) The processing of personal data shall be subject to the prior, free, informed, specific and unambiguous consent of the data subject.

(2) However, the requirement of prior consent may be waived where such processing is necessary in order to:

- comply with an obligation that is legally binding upon the controller;
- perform a public interest task or one falling within the remit of the Personal Data Protection Authority, entrusted to the controller or to the third party to whom the data are disclosed;
- preserve the health of the person concerned or of another natural person.

(3) The consent of a person aged under eighteen (18) years shall be valid only where it is supported by that of his/her father and mother or legal representative.

SECTION 10: The processing of personal data shall be legal, fair and non-fraudulent.

SECTION 11: Personal data must be collected only for specified, explicit and legitimate purposes and may not be further processed in a way that is incompatible with those purposes.

SECTION 12: Personal data must be complete, reliable and up to date. any person processing personal data shall be required to correct or delete any inaccurate or incomplete data.

SECTION 13: (1) Personal data shall be kept for no longer than is necessary for their processing.

(2) The period of retention of personal data referred to in (1) above shall be specified in the authorization to process data, under the conditions laid down by regulation.

(3) Beyond the period specified in (1) above, personal data may only be retained for historical, statistical or research purposes, in accordance with legal provisions in force.

SECTION 14: The controller must provide the data subject with clear and transparent information about the personal data processed.

SECTION 15: Personal data shall be processed by the controller in a confidential and secure manner, in particular where data transmission is involved.

SECTION 16: (1) Any processor who processes personal data on behalf of a controller shall provide sufficient guarantees of compliance with the security measures specified in this Act.

(2) The controller shall ensure that the processor complies with these measures.

SECTION 17: The controller or processor shall process personal data without regard to the social class, ethnic or regional origin, trade union membership, political opinions or religious beliefs of the data subject.

SECTION 18: The processing of personal data of minors for the provision of services must be appropriate, relevant and limited to what is necessary for the purposes for which it is processed.

CHAPTER II
FORMALITIES PRIOR TO THE PROCESSING OF PERSONAL DATA

SECTION 19: (1) The processing of personal data shall be subject to prior authorization by the Personal Data Protection Authority.

(2) Any interconnection and interoperability of files containing sensitive data relating to minors shall be subject to prior authorization by the Personal Data Protection Authority.

(3) The conditions for granting the authorization referred to in (1) and (2) above shall be laid down by regulation.

CHAPTER III
OBLIGATIONS OF THE CONTROLLER AND PROCESSOR

SECTION 20: The controller and processor shall be bound by the same obligations regarding the processing of personal data.

SECTION 21: The controller must provide the data subject with the following information at the time of collection and by any means:

- his/her identity;
- the purposes of the processing for which the data are intended;
- the categories of data concerned;
- the recipients to whom the data may be disclosed;
- the possibility to refuse to be included in the file in question;
- the existence of the right:

- to access personal data in accordance with the provisions of this law;
- to rectify, delete, object to, limit and transfer data;
- to be informed in the event of processing for commercial prospecting purposes;
- not to be the subject of an automated individual decision, including profiling;
- to be informed about an automated decision, the underlying reason and the expected consequences of the processing;
- to refuse disclosure of one's personal data to a third party;
- to determine post-motem processing guidelines;
- to lodge a complaint with the Personal Data Protection Authority;

- the duration of data retention;
- the possibility to transfer data to a foreign country.

SECTION 22: (1) Once the controller or processor are aware of a personal data breach, he/she must immediately inform the Personal Data Protection Authority and the data subject.

(2) In any case, and without prejudice to the provisions of (1) above, the controller or processor shall be required to implement appropriate technical and organizational security measures such as encryption and restrictive access authorization.

SECTION 23: (1) The controller or processor of personal data shall take all necessary measures to inform all data subjects of a request for erasure.

(2) In the case referred to in (1) above, the controller or processor shall put in place appropriate mechanisms to guarantee the right to digital oblivion or erasure of the data concerned.

(3) The controller and processor shall be jointly and severally liable for any disclosure of personal data without the consent of the data subject.

SECTION 24: (1) The controller or processor shall process personal data in a confidential manner.

(2) Personal data shall be processed only by persons acting under the authority of the controller and only on his instructions.

(3) The controller shall implement technical and organizational measures when determining processing methods and during processing proper, which shall be recorded in the benchmark established by the Personal Data Protection Authority.

SECTION 25: (1) The controller and processor shall assess personal data processing risks based on the assessment criteria and review and validation procedures laid down by regulation.

(2) The controller and processor shall take all the necessary measures to prevent, in particular:

- the deformation, damage or unavailability of the data;

- unauthorized access to them by third parties.

(3) The controller and processor shall ensure that any person acting under their respective authority who has access to personal data processes them in accordance with the instructions and for the purposes specified.

SECTION 26: Every processor shall provide sufficient guarantees for the technical and organizational security measures related to the processing to be carried out.

SECTION 27: (1) The controller and the processor of personal data shall be bound to:

- ensure the availability of personal data, in particular by implementing measures to ensure the resilience of personal data information systems;
- ensure that where an automated data processing system is used, authorized persons can access only data within the scope of their authorization;
- ensure that the identity of third parties to whom data may be transferred are checked and confirmed;
- ensure that the identity of persons who can access the personal data information system, the type of data entered, modified, altered, copied, erased or read in the system and the period when such data were processed are pre-checked and pre-confirmed;
- prevent unauthorized access to data processing equipment;
- prevent data media from being read, copied, modified or relocated by unauthorized persons;
- prevent the unauthorized introduction of data into the information system and the unauthorized access, modification or erasure of recorded data;
- prevent the use of data processing systems by unauthorized persons using data transmission equipment;
- protect data by making secure back-up copies;
- take any other appropriate measures provided for by regulation.

(2) The data controller shall submit an annual report to the Personal Data Protection Authority on the status of implementation of the security measures contained in the technical and organizational measures benchmark.

SECTION 28: The maximum period for which personal data may be kept shall be laid down by the data protection authority within the benchmark provided for in the previous section. This period shall be determined taking into account the purpose of the processing or the nature of the data collected, in accordance with the laws and regulations in force.

SECTION 29: (1) The controller or processor shall keep a physical or digital register of the processing operations carried out under his/her responsibility

(2) The register referred to in (1) above shall contain the following information:

- the name and contact details of the controller and, where applicable, the name of the processor;

- the purposes of processing the data;
- a description of the categories of data subjects and personal data.
- the categories of recipients to whom the personal data have been or will be disclosed;
- documents attesting to the existence of appropriate safeguards or the number of the authorization issued by the Personal Data Protection Authority.

SECTION 30: (1) Where the controller has recourse to a processor, he/she shall ensure that the latter has sufficient guarantees regarding the implementation of appropriate technical and organizational measures so that the processing complies with the requirements of this law.

(2) The processing of personal data by a processor shall be governed by a contract between the processor and the controller.

(3) The contract referred to in (2) above shall specify, in particular, the type of personal data and the categories of data subjects concerned, as well as the responsibilities and rights of the controller and processor.

SECTION 31: (1) In the case of joint processing, controllers shall determine the purposes and methods of processing and shall be jointly and severally liable for them.

(2) The joint controllers shall clearly state, by means of an agreement which shall be made public, their respective obligations to ensure compliance with the requirements of this law, particularly their respective roles, relationship with the data subject, the exercise of the rights of the data subject, as well as their respective obligations regarding disclosure of the information referred to in Section 26 of this law.

(3) Notwithstanding the terms of the agreement referred to in (2) above, the data subject shall exercise the rights conferred on him/her by this law vis-à-vis the controllers.

SECTION 32: (1) The transfer of personal data to a foreign country or to an international organization shall be subject to the prior authorization of the Personal Data Protection Authority under conditions which guarantee the exercise of the rights of the data subject.

(2) In granting such authorization, the Personal Data Protection Authority shall first ensure that:

- the country of destination of the personal data provides an adequate level of protection;
- the prior entry into force of a legal instrument signed with the country of destination of the personal data transferred, in conjunction with the relevant ministries and bodies;
- that the entity requesting the import of personal data is subject to binding security rules on the protection of such data;
- prior compliance by the importing and exporting entities concerned with the standard contractual clauses for the international transfer of personal data drafted and published by the Personal Data Protection Authority.

(3) The conditions for granting the authorization referred to in (1) above shall be laid down by regulation.

SECTION 33: (1) All data processing operations likely to entail a high risk for the rights and freedoms of individuals shall be subject to a prior assessment of the impact of the intended processing operations on the protection of personal data.

(2) The terms and conditions for carrying out the impact assessment referred to in (1) above shall be laid down by regulation.

SECTION 34: The Personal Data Protection Authority shall establish a mechanism for certifying the processing of personal data in accordance with the principles and requirements provided for in this law.

SECTION 35: The conditions for monitoring and controlling the implementation of the obligations of the controller and processor shall be laid down by regulation.

CHAPTER VI
INTERCONNECTION OF FILES

SECTION 36: (1) The interconnection of files shall be lawful only where it is necessary to comply with a legal obligation by which the controller is bound.

(2) It should not lead to discrimination or limit the rights, freedoms and guarantees of data subjects and should include appropriate security measures and take into account, where applicable, the principle of minimization of the data to be interconnected.

PART III
RIGHTS OF THE DATA SUBJECT

SECTION 37: Any data subject may request the controller to stop disclosing and to erase his/her data, under the conditions provided for in this law and separate implementing instruments thereof.

SECTION 38: (1) The data subject shall have the right to request the controller to stop disclosing and to erase his/her data for any of the following reasons:

- the purpose for which the data were processed is no longer relevant;
- the consent on which the processing is based has been vitiated, withdrawn or has expired;
- there is no legal basis for the processing; or
- any other reason provided for by law.

(2) The controller shall erase personal data immediately upon the express request of the data subject in the circumstances referred to in (1) above, subject to the requirements for personal data retention, in accordance with the provisions of this law and those of the laws and regulations in force.

SECTION 39: The data subject may request from the controller:

- information that would enable him to be aware of the processing and to object to it;
- confirmation as to whether or not personal data concerning him/her are being processed;
- communication of the personal data concerning him/her and of any information available as to its source;
- information about the purpose of the processing, the categories of personal data processed and the recipients or categories of recipients to whom the data are disclosed;
- a copy of his/her personal data in an intelligible form for an amount not exceeding the cost of reproduction.

SECTION 40: (1) Any data subject shall have the right to object at any time to the processing of his/her personal data for any of the following reasons:

- any reason relating to the processing of special categories of personal data;
- any processing for prospecting purposes;
- any other reason provided for by the law in force.

(2) When using information society services, the data subject may exercise his/her right to object by means of automated procedures using technical specifications.

(3) The parent or legal representative of a minor child shall have the right to object to the processing of personal data relating to the minor which have been collected without his/her consent.

(4) If the data subject objects to the processing of his/her data for commercial marketing purposes, the data may no longer be used for such purposes.

SECTION 41: (1) The disclosure of personal data to third parties or their use on behalf of third parties for direct marketing purposes shall be subject to the prior consent of the data subject.

(2) The consent referred to in (1) above shall be given after the data subject has been informed in accordance with the provisions of this law.

SECTION 42: Any natural person who can justify his/her identity may request the controller of a processing operation to rectify, complete, update, block or delete inaccurate or incomplete personal data concerning him/her.

SECTION 43: (1) The data subject shall have the right to obtain, free of charge, the personal data relating to him/her which are held by a controller in a structured, commonly used and machine-readable format.

(2) The data subject shall have the right to data portability.

(3) Where the data subject exercises his/her right to data portability under (1) above, he/she shall have the right to have his/her personal data transferred directly from one controller to another, where technically possible.

(4) The right to data portability shall not apply to data processed for public interest purposes or for the exercise of official authority vested in the controller.

SECTION 44: (1) The data subject shall have the right to object to any decision based solely on the automated processing of his personal data, including profiling.

(2) The provisions of (1) above shall not apply where:

- the data subject is informed of the use of the automated decision making system and has given his/her prior, explicit and informed consent;
- processing is permitted by law, provided that it lays down appropriate measures to safeguard the rights and freedoms and legitimate interests of the data subject.

(3) The data subject shall also have the right to:

- obtain human intervention from the controller;
- express his/her point of view;
- challenge any decision based on automated processing.

SECTION 45: (1) The processing of personal data relating to a natural person shall cease when that person dies.

(2) However, a person's personal data may be kept after his/her death:

- where this is a legally binding obligation on the controller;
- for the purpose of defending the interests of the controller in legal proceedings, pending the resolution of such proceedings;
- where the data subject has provided the controller with general post-mortem instructions for the processing of his/her personal data.

(3) The rightful claimants of a deceased person may request, at the expense of the controller, that the information concerning the deceased person be updated.

SECTION 46: (1) Any data subject shall have the right to obtain from the controller restriction of the processing where the accuracy of the personal data or the purpose of the processing is contested.

(2) Where processing has been restricted in accordance with (1) above, personal data may be processed, except for their conservation, only with the consent of the data subject or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person.

SECTION 47: The time limits and procedures for review of requests from data subjects relating to the exercise of their rights under this law shall be laid down by regulation.

PART IV
PROHIBITIONS ON THE PROCESSING OF PERSONAL DATA

SECTION 48: (1) The processing of data relating to religious, philosophical, political or trade-union opinions and activities, to racial or ethnic origin, to linguistic or regional origin, to genetics and to health biometrics shall be prohibited.

(2) The processing of personal data in connection with banking transactions shall be prohibited without the prior authorisation of the competent public authorities and bodies, under the terms and conditions laid down by the laws in force.

SECTION 49: It shall be prohibited to process personal data without the prior authorization of the relevant government services and entities, under the terms and conditions provided for in this law.

SECTION 50: The processing of personal data without the prior consent of the data subject shall be prohibited.

SECTION 51: The processing of personal data shall be prohibited:

- where the erasure of such data has been ordered by the Personal Data Protection Authority;
- where it is contrary to public order, morality, or the interests of the national community.

SECTION 52: The processing of personal data shall not undermine human dignity and identity, individual and collective freedoms or human rights in general, as recognized by applicable legislation and duly ratified international conventions.

PART V
PERSONAL DATA PROTECTION AUTHORITY

SECTION 53: (1) The Personal Data Protection Authority shall be an independent public body responsible, in particular, for:

- ensuring the implementation of this law, its enabling instruments and relevant international agreements;
- issuing the authorizations provided for in this law, including relevant specifications;
- preparing, publishing and updating the personal data benchmark of technical and organizational measures;
- approving certification mechanisms for personal data processing procedures and techniques;
- handling complaints, petitions and enquiries submitted by a data subject or by a body, organization or association and, where necessary, review or investigate the subject of such complaints, petitions or enquiries and inform the claimant, petitioner or complainant of the progress and outcome of the investigation within a reasonable time;
- drawing up and publishing a list of countries recognised as offering a level of protection of personal data equivalent to that required by Cameroonian law;
- cooperating with other authorities responsible for the protection of personal data, in conjunction with the relevant ministries and entities;

(2) A decree of the President of the Republic shall lay down the establishment, organization and functioning of the Personal Data Protection Authority referred to in (1) above.

PART VI
SANCTIONS

CHAPTER I
ADMINISTRATIVE SANCTIONS

SECTION 54: (1) Where the Personal Data Protection Authority finds that the controller or processor has failed to comply with its obligations, it shall give the controller or processor formal notice to comply within a maximum period of ten (10) days.

(2) Beyond the period provided for in (1) above, the Personal Data Protection Authority shall issue an injunction to ensure compliance of processing, subject to a fine of up to 100 000 (one hundred thousand) CFA francs per day of delay.

(3) Where the controller or processor fails to comply with the formal notice provided for in (1) above, the Personal Data Protection Authority may inflict one of the following sanctions:

- suspension of the activity for which authorization was granted;
- withdrawal of the authorization;
- prohibition from carrying out any activity involving the processing of personal data.

SECTION 55: Without prejudice to the penalties provided for in Section 54 above, whoever engages in the processing of personal data without prior authorization shall be punished with a fine of from 5 000 000 (five million) to 50 000 000 (fifty million) CFA francs.

SECTION 56: Any controller or processor who refuses to provide the data subject with the information requested concerning him/her shall be punished with a fine of from 1 000 000 (one million) to 10 000 000 (ten million) CFA francs.

SECTION 57: Any controller or processor who fails to comply with the provisions of the benchmark provided for in this law shall be punished with a fine of from 5 000 000 (five million) to 20 000 000 (twenty million) CFA francs.

SECTION 58: Any controller or processor who fails to comply with the provisions relating to the interconnection of files as provided for in this law shall be punished with a fine of from 1 000 000 (one million) to 5 000 000 (five million) CFA francs.

SECTION 59: Any controller or processor operating without the certification provided for in this law shall be punished with a fine of from 5 000 000 (five million) to 15 000 000 (fifteen million) CFA francs.

SECTION 60: Any controller or processor who transfers personal data to a third country without the prior authorization of the Personal Data Protection Authority shall be punished with a fine of from 10 000 000 (ten million) to 50 000 000 (fifty million) CFA francs.

SECTION 61: Any data controller or processor who fails to comply with any of the obligations set out in the specifications shall be punished with a fine of from 10 000 000 (ten million) to 100 000 000 (one hundred million) CFA francs.

CHAPTER II
CIVIL AND PENAL PENALTIES

I - CIVIL PENALTIES

SECTION 62: (1) In the event of serious infringement of the rights referred to in this law, the data subject may petition the competent court ruling under the emergency procedure, to order, as and when necessary, under penalty of law, any measure necessary to safeguard his/her right.

(2) The data subject may apply to the competent court for compensation.

II- PENAL SANCTIONS

SECTION 63: (1) Whoever collects or accesses personal data by fraudulent, unfair or unlawful means shall be punished with imprisonment for from 2 (two) to 5 (five) years or a fine of from 200 000 (two hundred thousand) to 5 000 000 (five million) CFA francs, or both such imprisonment and fine.

(2) The penalties provided for in (1) shall be doubled where the collection or access by fraudulent means involves blocking, encryption or any other technique that undermines data availability and integrity.

SECTION 64: (1) Any controller or processor who processes or commissions the processing of personal data despite the objection of the data subject, where such processing is intended for direct prospecting or where the objection is provided for by law, shall be punished with imprisonment for from 1 (one) to 3 (three) years or a fine of from 50 000 (fifty thousand) to 1 000 000 (one million) CFA francs, or both such imprisonment and fine.

(2) Any controller or processor who fails to carry out or to commission the operations requested by a natural person who can identify himself/herself and who requests that personal data concerning him/her or a deceased person for whom he/she is the legal representative or beneficiary be rectified, completed, updated, blocked or erased shall be liable to the penalties provided for in (1) above.

SECTION 65: Any controller or processor who processes or commissions the processing of personal data for the purpose of profiling shall be punished with imprisonment for from 3 (three) to 10 (ten) years or a fine of from 1 000 000 (one million) to 20 000 000 (twenty million) CFA francs, or both such imprisonment and fine.

SECTION 66: (1) Any controller or processor of personal data who, without the express consent of the data subject, saves or stores sensitive data within the meaning of this law, whether electronically or not, shall be punished with imprisonment for from 6 (six) months to 2 (two) years or a fine of from 500 000 (five hundred thousand) to 5 000 000 (five million) CFA francs, or both such imprisonment and fine.

(2) Whoever fraudulently recovers or commissions the recovery of deleted personal data shall be liable to the penalties provided for in (1) above.

SECTION 67: The following shall be punished with imprisonment for from 6 (six) months to 2 (two) years or a fine of from 500 000 (five hundred thousand) to 5 000 000 (five million) CFA francs, or both such imprisonment and fine:

- the controller or processor who, in the course of recording, filing, transmitting or any other form of processing, diverts the information from its original purpose;
- the controller or processor who subsequently processes or commissions the further processing of personal data incompatible with the original purpose.

SECTION 68: (1) Whoever collects, classifies, transmits or otherwise processes personal data whose disclosure would either undermine the dignity or privacy of the person concerned, or who discloses such data to a third party without the consent of the person concerned, shall be punished with imprisonment for from 6 (six) months to 2 (two) years or a fine of from 200 000 (two hundred thousand) to 5 000 000 (five million) CFA francs, or both such imprisonment and fine.

(2) In the case referred to in (1) above, proceedings may be initiated only on the basis of a complaint by the victim, his/her legal representative or his/her beneficiaries.

SECTION 69: Whoever, in violation of the provisions of this law, transfers or causes to be transferred to a foreign State or an international organization personal data which are or are intended to be processed, shall be punished with imprisonment for from 3 (three) to 10 (ten) years or a fine of from 2 000 000 (two million) to 20 000 000 (twenty million) CFA francs, or both such imprisonment and fine.

SECTION 70: (1) Any controller or processor who obstructs the action of the Personal Data Protection Authority:

- by preventing the performance of the tasks entrusted to its staff or agents on official mission; or
- by refusing to provide the staff or agents of the Personal Data Protection Authority on official mission with the information or documents they need to perform their duties.

shall be punished with imprisonment for from 6 (six) months to 3 (three) years or a fine of from 100 000 (one hundred thousand) to 500 000 (five hundred thousand) CFA francs, or both such imprisonment and fine:

(2) The penalties provided for in (1) above shall be doubled where the said documents or information are concealed, falsified or deleted.

SECTION 71: Without prejudice to the criminal liability of their officials, legal persons may be declared criminally liable to and punished with a fine of from 50 000 000 (fifty million) and 1 000 000 000 (one billion) CFA francs, where the offences provided for by this law are committed by officials of the said legal persons.

PART VII
MISCELLANEOUS, TRANSITIONAL AND FINAL PROVISIONS

SECTION 72: The processing of personal data relating, in particular, to security, defence, health, justice and civil status shall, as and when necessary, be governed, by separate instruments.

SECTION 73: Natural or legal persons responsible for the processing of personal data shall have 18 (eighteen) months from the date of enactment of this law to comply with its provisions.

SECTION 74: The conditions for the implementation of this law shall be laid down, as and when necessary, in separate instruments.

SECTION 75: This law, which repeals all previous provisions repugnant hereto, shall be registered, published according to the procedure of urgency and inserted in the Official Gazette in English and French./-

PRESIDENCE DE LA REPUBLIQUE
PRESIDENCY OF THE REPUBLIC
SECRETARIAT GENERAL
SERVICE DU FICHIER LEGISLATIF ET REGLEMENTAIRE
LEGISLATIVE AND STATUTORY AFFAIRS CARD INDEX SERVICE
COPIE CERTIFIEE CONFORME
CERTIFIED TRUE COPY

YAOUNDE, 23 DEC 2024

REPUBLIQUE DU CAMEROUN
PAIX-TRAVAIL-PATRIE
LE PRESIDENT
THE PRESIDENT
PEACE-WORK-FATHERLAND

PAUL BIYA
PRESIDENT OF THE REPUBLIC