LAW Nº ……..…/2020 OF …...……. /……...../…… ON DATA PROTECTION AND PRIVACY

We, KAGAME Paul,

President of the Republic;

THE PARLIAMENT HAS ADOPTED AND WE SANCTION, PROMULGATE THE FOLLOWING LAW AND ORDER IT BE PUBLISHED IN THE OFFICIAL GAZETTE OF THE REPUBLIC OF RWANDA

THE PARLIAMENT:

The Chamber of Deputies, in its session of ……;

Pursuant to the Constitution of the Republic of Rwanda of 2003 revised in 2015, especially in Articles 23, 64, 69, 70, 88, 90, 91, 106, 120 and 176;

Pursuant to the presidential order nº 024/2019 of 04/09/2019 ratifying the African Union Convention on Cyber Security and Personal Data Protection;

ADOPTS:

Table of Contents

CHAPTER I: GENERAL PROVISIONS

Article 1: Purpose of this Law

The purpose of this law is:

i. to provide mechanisms through which the protection and privacy of personal data will be ensured in connection with its processing in Rwanda.

ii. to ensure the free flow of non-personal data within and outside Rwanda by laying down rules relating its protection.

Article 2: Scope of this Law

This law shall apply to any person who processes data whether:

i. Done by electronic or other means using data through an automated or non-automated platform, forming or intending to form part of a filing system;

ii. Established or ordinarily resident in Rwanda that processes data while in Rwanda; or

iii. Not established or not ordinarily resident in Rwanda, but processing personal data of data subjects located in Rwanda.

iv. Non-personal data is provided as a service to users residing or having an establishment in Rwanda.

<u>Article 3.</u> Definition of Terms

For the purpose of this Law, the following terms shall be defined as follows:

1. **Competent authority**: sectorial authorities with data under their mandate;
2. **Consent of the data subject:** any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
3. **Confidential:** data that might be less restrictive within the entity but might cause damage if disclosed;
4. **Data:** information which:
   (a) is processed by means of equipment operating automatically in response to instructions given for that purpose;
   (b) is recorded with the intention that it should be processed by means of such equipment;
   (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; or
   (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record;
5. **Data breach**: a violation of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;
6. **Data controller**: a natural person, moral person (either public or private) or any other body which, alone or jointly with others, collects and/or determines the purposes and means of the processing of personal data;

7. **Data embassy**: a physical or virtual data center in an allied foreign country that stores data of critical government information systems and mirrors of critical service applications;
8. **Data processor:** a natural person, moral person (either public or private) or any other body authorized by the data controller to process personal data;
9. **Data processing**: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, analysis, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
10. **Data subject**: an individual from whom or in respect of whom personal information has been requested, collected, collated, processed or stored;
11. **Encryption:** the process of converting the content of any readable data using technical means into coded form;
12. **Open data**: open to the general public with no restrictions;
13. **Person:** any natural or moral person
14. **Personal data:** any information relating to an identified or identifiable data subject;
15. **Profiling**: any form of automated processing of personal data involving the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyze or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;
16. **Pseudonymization**: the processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such

additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data cannot be attributed to an identified or identifiable individual;

17. **Privacy**: a fundamental right of a person to decide who, when, why, where, what and how his/her personal data can be accessed.
18. **Recipient**: a natural person, moral person or any other body, to which the personal data are disclosed, whether a third party or not;
19. **Secret:** data of which unauthorized disclosure would cause serious damage to the national security. This data is considered less sensitive than data classified as top secret;
20. **Sensitive personal data**: data revealing the natural person's race, traffic data, health status, criminal or medical records, social origin, religious or philosophical beliefs, political opinion, genetic data, biometric data, property or financial details, family details including names of the person's children, parents, spouse or spouses, sex, sexual life or orientation of the data subject;
21. **Tokenization:** the process of replacing sensitive data with unique identification symbols that retain all the essential information about the data without compromising its security
22. **Top secret:** data of which unauthorized disclosure would cause severe damage to the national security;
23. **Third party**: any natural person, moral person or any other body other than the data subject, data controller, processor and persons who, under the direct authority of the data controller are authorized to process personal data;
24. **User**: a natural person, moral person (either public or private) or any other body, using or requesting non-personal data processing service;
25. **Vital interests**: interest linked to life and/or death of data subject.

<u>Article 4:</u> Data categorization and classification

For the purpose of this Law, the data shall be categorized as personal data and non-personal data;

Personal data shall be classified as sensitive and non-sensitive data. Non-personal data shall be classified as top secret, secret, confidential and open data.

<u>Article 5:</u> Principles of data protection

The following principles of data protection shall apply to any information concerning a data subject;

a) **Lawfulness, fairness:** The processing of personal data shall be undertaken lawfully, fairly and non-fraudulently.

b) **Openness**: Individuals should be able to avail themselves of data collection and be able to contact the entity collecting this information.

c) **Purpose limitation:** Personal data must only be collected for a specific, explicit and legitimate purpose.

d) **Data minimization:** Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

e) **Data quality:** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

f) **Storage limitation:** Personal data must be kept in a form which permits identification of data subjects for no longer than is

necessary for the purposes for which the personal data are processed;

g) **Confidentiality and integrity:** Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

h) **Accountability:** The data controller shall be responsible and be able to demonstrate compliance with the above principles

CHAPTER II: GENERAL RULES FOR COLLECTING AND PROCESSING PERSONAL DATA

Section One: General Rules

Article 6: Privacy of the data subject

A data controller, data processor and any involved third party shall collect, hold or process personal data in a manner which does not infringe the privacy of the data subject.

Article 7: Consent to collect or process personal data

The controller shall bear the burden of proof for establishing a data subject's consent to the collecting and/or processing of his/her personal data for a specified purpose.

Consent is effective only when it is based on the data subject's free decision. The data subject shall be informed in advance of the consequence of his or her consent.

The consent may be given in a form of a written statement including electronic means, or oral statement.

Article 8: Declaration of consent

The data subject's consent given in the context of a written declaration, which also contains other matters, shall be presented in a manner which is clearly distinguishable from those other matters, in an intelligible and easily accessible from using a clear, plain and understandable official language to the data subject.

Any part of such a declaration which constitutes an infringement to the provision of this Law shall not be binding.

Article 9: Right to withdraw

The data subject has full right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Prior to giving consent, the data subject shall be informed thereof. The withdrawal shall be as easy as giving consent.

Article 10: Child's consent

The processing of the personal data of a child shall be lawful where the child, is at least 16 years old. Where the child is below that age, such processing shall be lawful only when it is given by either both parents or the legal guardian.

Article 11: Grounds for collecting and processing sensitive personal data

Sensitive personal data shall not be collected and processed unless:

(a) processing is necessary for the purposes of carrying out the obligations of the data controller or data processor, or exercising specific rights of the data subject, in accordance with applicable Laws;

(b) processing is necessary to protect the vital interests of the data subject or of another individual;

(c) processing is necessary for the purposes of preventive or occupational medicine, public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices;

(d) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Article 12: Safeguards to process sensitive personal data

If sensitive personal data are processed, appropriate safeguards for the legally protected interests of the data subject must be set. These safeguards include but not limited to:

(a) specific requirements for data security or data protection monitoring;
(b) special time limits within which data must be reviewed for relevance and erasure;
(c) measures to increase awareness of staff involved in processing operations;
(d) restrictions on access to sensitive personal data within the controller;
(e) separate processing of such data;
(f) the tokenization of sensitive personal data;
(g) the pseudonymization of sensitive personal data;
(h) the encryption of sensitive personal data; or
(i) Specific codes of conduct to ensure lawful processing in case of transfer or processing for other purposes.

Article 13: Processing personal data relating to criminal convictions

Processing of personal data relating to criminal convictions and offences shall be carried out under the control of the competent Authority or when the processing is authorized by law into force, the processor must provide appropriate safeguards for the rights and freedoms of data subject.

Article 14: Processing which does not require identification

If the purposes for which personal data is processed do not or no longer require the identification of a data subject, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Law.

Where, in cases referred to in paragraph (1) of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 23 to 28 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

Article 15: Source of personal data

Any person who intends to collect personal data, shall collect it directly from the data subject.

However, personal data may be collected from another person, source or public body, where:

(a) the data is contained in a public record;
(b) the data subject has deliberately made the data public;

(c) the data subject has consented to the collection of the information from another source;
(d) the collection of the data from another source is not likely to prejudice the privacy of the data subject;
(e) the collection of the data from another source is lawfully justified.

Article 16: Information to be given to data subject before collection of personal data

Any person collecting personal data shall inform the data subject of the following:

(a) The nature and category of the data being collected;
(b) The name and address of the person responsible for the collection and the purpose for which the data is required;
(c) Whether or not the supply of the data by the data subject is discretionary or mandatory;
(d) The effects of not providing the data;
(e) The authorization or the requirement by law for the collection of data
(f) The recipients of the data;
(g) The exercise of the right of access to and right to request rectification of the data collected where applicable;
(h) The period for which the data will be retained to achieve the purpose for which it is collected.

Where the data is collected from a third party for purposes other than public interest, the data subject shall be given the information specified above, before the collection of the data.

Section 2: Quality Information and Record of Personal Data

Article 17. Personal data quality

The data controller or data processor shall ensure that the personal data is complete, accurate, up-to-date and not misleading, having regard to the purpose for its collection or processing.

Article 18. Correction, deletion and destruction of personal data

The data subject may request the data controller or data processor to:

(a) Correct or delete personal data in relation with the data subject held by or under the control of the data controller that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully;
(b) Destroy or delete record of personal data about the data subject held by the data controller which the data controller no longer has the authority to retain.

Upon receipt and analysis of the request for corrections, deletion or destruction of personal data, the data controller shall respond to the request and inform thereof in a written form within fifteen (15) working days from the date of reception.

Where the data controller complies with the request, the data controller shall inform each person to whom the personal data has been disclosed of the action taken whether correction, deletion or destruction.

Article 19: Logging

The data controllers and data processors shall provide for logs to be kept for at least the following processing operations in automated processing systems:

(a) collection,
(b) alteration,
(c) consultation,
(d) disclosure including sharing and transfers,
(e) combination, and
(f) Erasure.

The logs of consultation and disclosure must make it possible to ascertain the justification, date and time of such operations and, as far as possible, the identity of the person who consulted or disclosed personal data, and the identity of the recipients of the data.

The logs may be used only by the competent Authority or the data subject to verify the lawfulness of the processing; and for self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.

Article 20: Erasure of personal data

Any data controller or processor shall erase personal data without undue delay where:

(a) the data are no longer necessary in relation to the purpose for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;

(c) the data subject objects to the processing of personal data and there are no overriding legitimate grounds for the processing; or
(d) the personal data have been unlawfully processed.

Where the controller has made the personal data available on public domain, he/she shall take all reasonable steps to inform third parties processing such data, that the data subject has requested the erasure of any links to, or copy or replication of, that personal data.

However, erasure of personal data shall not apply where the processing of the personal data is necessary for:

(a) reasons of public interest in the field of public health;
(b) the purpose of historical, statistical or scientific research;
(c) compliance with a legal obligation to process the personal data to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
(d) The establishment, exercise or defense of a legal claim.

Article 21: Restriction of processing personal data

The data controller on his/her own initiative or under the request of the competent Authority or of the data subject, may restrict the processing of personal data for a given period where:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;
(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or

(c) The data subject has objected to the processing pending verification as to whether the legitimate grounds of the controller override those of the data subject.

Where processing of personal data is restricted:

(a) the personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defense of a legal claim, the protection of the rights of another person or for reasons of public interest; and

(b) The controller shall inform the data subject before lifting the restriction on processing of the personal data.

Article 22: Data processing records

Every controller or processor shall maintain a record of all processing operations under his/her or its responsibility.

The record shall set out:

(a) the name and contact details of the controller or processor, and, where applicable, his or its representative and any data protection officer;

(b) the purpose of the processing;

(c) a description of the categories of data subjects and of personal data;

(d) a description of the categories of recipients to whom personal data have been or will be disclosed, including recipients in other countries;

(e) any transfers of data to another country, and, in the case of a transfer referred to in article 53, the suitable safeguards;

(f) where possible, the envisaged time limits for the erasure of the

different categories of data; and

(g) the description of the mechanisms referred to in article 38 (3).

The controller or processor shall, on request, make the record of processing operations available to the Authority in charge of data protection and privacy.

CHAPTER III: RIGHTS OF THE DATA SUBJECT

Article 23: Right to information

Without prejudice to other relevant laws, the data subject may request a data controller or data processor to:

(a) provide the information relating to the purposes of the processing;
(b) provide a copy of the data about the data subject;
(c) give a description of the personal data which is held by the data controller including data about the identity of a third party or a category of a third party who has or has had access to the information;
(d) request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(e) be informed of the source of data where the personal data were not collected from the data subject;
(f) be informed in case personal data are transferred to a third country or to an international organization.

The data controller or data processor shall provide the information to the data subject in a clear and concise manner.

Article 24: Right to object

The data subject may at any time by notice in writing to the data controller and/or data processor require the data controller and/or data processor to stop processing personal data which causes or is likely to cause unwarranted substantial damage or distress to the data subject;

The data controller or data processor shall within a period of fifteen (15) working days after receipt of the notice inform the concerned data subject in writing about the compliance or the intention to comply with the notice, or of the reasons for non-compliance.

The data subject not satisfied by the response of the data controller and data processor may appeal to the Authority in charge of data protection and privacy.

Article 25: Right of rectification or erasure

The data subject may demand that the data controller rectify, complete, update, block or erase, as the case may be, the personal data concerning him/her where such data are inaccurate, incomplete, equivocal or out of date, or whose collection, use, disclosure or storage are prohibited.

Article 26: Right to data portability

The data subject may request transfer or sharing of his/her personal data from one data controller to another.

Article 27: Automated individual decision-making

Any data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him/her or significantly affects him/her.

However, this right shall not apply where the decision is:

(a) necessary for entering into, or performing, a contract between the data subject and a controller;
(b) authorized by a law or a regulation into force to which the controller is subject and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or
(c) Based on the data subject's explicit consent.

Any automated processing of personal data intended to evaluate certain personal aspects relating to an individual shall not be based on sensitive personal data.

Article 28: Exercise of rights by representation

Any right by representation conferred on the Data subject may be exercised:

(a) where the data subject is a minor, by a person who has parental authority over the minor or has been appointed as his/her guardian;
(b) where the data subject is physically or mentally unfit, by a person who has been appointed as his/her guardian or legal administrator by a Court; or
(c) in any other case, by a person duly authorizedin writing by the data subject to make a request under this chapter.

Article 29: Personal data of a deceased person

Heirs are entitled to access, request deletion and rectification of the relevant data from data controllers and processors, unless deletion or rectification was prohibited by the deceased individual or by applicable law.

CHAPTER IV: REGISTRATION OF DATA CONTROLLER AND DATA PROCESSOR

Article 30: Controller and Processor

Any person who intends to act as controller or processor shall first register with the authority in charge of personal data protection and privacy.

The Authority in charge of data protection and privacy shall prescribe thresholds required for mandatory registration by considering the nature of industry, volumes of data processed, whether it is a sensitive personal data and any other criteria as the Authority in charge of data protection and privacy under this article may specify.

Article 31: Application for registration

Every person who intends to act as a controller or processor shall apply to the authority in charge of data protection and privacy which may approve such registration.

Every application under paragraph (1) shall be accompanied by the following particulars regarding the applicant:

(a) name and address;

(b) if he/she or it has nominated a representative for the purposes of this Law, the name and address of the representative;

(c) a description of the personal data to be processed by the controller or processor, and of the category of data subjects, to which the personal data relate;

(d) a statement as to whether or not he/she or it holds, or is likely to hold, special categories of personal data;

(e) a description of the purpose for which the personal data are to be processed;

(f) a description of any recipient to whom the controller intends or may wish to disclose the personal data;

(g) the name, or a description of, any country to which the proposed controller intends or may wish, directly or indirectly, to transfer the data;

(h) a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of the personal data; and

(i) Any other requirement as may be determined by the authority in charge of data protection and privacy.

The Authority in charge of data protection and privacy determines the modalities for registration of public institutions who have collection and processing of personal data within their competencies.

Article 32: Issuance of registration certificate

Where the Authority in charge of data protection and privacy considers that an applicant meets the criteria to be registered as a controller or processor, as the case may be, it shall grant the registration certificate.

The registration modalities and validity period of the registration certificate shall be determined by the Authority in charge of personal data protection and privacy.

Article 33: Change in particulars

Where, following the grant of registration certificate, there is a change in any of the particulars referred to in article 30, paragraph (2), the

controller or processor shall, within fifteen (15) working days, notify the Authority in charge of data protection and privacy in writing of the nature and date of the change.

On receipt of a notification under paragraph (1), the Authority in charge of data protection and privacy, on being satisfied that there is a change in particulars, shall amend the appropriate entry in the register.

Article 34: Renewal of registration certificate

The holder of a registration certificate may apply for the renewal of the certificate not later than three (3) months before the date of its expiry.

The request for renewal of the registration certificate shall be granted under terms and conditions as may be determined by the Authority in charge of data protection and privacy.

Article 35: Cancellation or modification of registration certificate

The modification of registration certificate may be initiated by the Authority in charge of data protection and privacy or at the request of the holder.

The Authority in charge of data protection and privacy may modify the certificate before its expiration when it determines that modification is needed to respond to:

i. Significant change on applicable laws;

ii. Inability of the certificate holder to comply with terms and conditions beyond his/her control.

iii. Any change in particulars that may affect the registration certificate.

The Authority in charge of data protection and privacy may cancel the registration certificate before its expiration due to:

(a) any information given to him by the applicant is false or misleading in any material particular;

(b) the holder of the registration certificate fails, without lawful excuse, to comply with:

(i) any requirement of this Law; or

(ii) any term or condition specified in the certificate.

Prior cancellation of the registration certificate the authority in charge of data protection and privacy shall provide the cancellation notice to the certificate holder requesting him/her to provide explanations on the non-compliance of paragraph (3) within fifteen (15) working days.

Article 36: Register of controllers and processors

There shall be a register of controllers and processors to be known as the Data Protection Register, which shall be kept and maintained by the Authority in charge of data protection and privacy in such form and manner as it may determine.

The Authority in charge of data protection and privacy may, at any time, at the request of a controller or processor, in respect of which there is an entry in the register and which has ceased to exist, remove its details from the register.

The Authority in charge of data protection and privacy shall determine the modalities under which the register shall, at all reasonable times, be available for consultation.

Any person may obtain from the Authority in charge of data protection and privacy a certified copy of, or of an extract from, any entry in the register.

CHAPTER V: OBLIGATIONS AND DUTIES OF DATA CONTROLLER AND DATA PROCESSOR

Article 37: Obligations relating to processing of personal data

Every controller or processor shall ensure that personal data are:

(a) processed lawfully, fairly and in a transparent manner in relation to any data subject;

(b) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and

(f) processed in accordance with the rights of data subjects.

Article 38: Duties of data controller

Every controller shall adopt policies and implement appropriate technical and organizational measures so as to ensure and be able to demonstrate that the processing of personal data is performed in accordance with this Law.

The measures referred to in paragraph (1) of this article shall include:

(a) implementing appropriate data security and organizational

measures;

(b) keeping a record of all processing operations;

(c) performing a data protection impact assessment;

(d) complying with the requirements for prior authorization from, or consultation with the Authority; and

(e) designating an officer responsible for data protection compliance issues.

Every controller shall implement such policies and mechanisms as may be required to ensure verification of the effectiveness of the measures referred to in this article.

Article 39: Collection of Personal Data

A controller shall not collect personal data unless:

(a) it is done for a lawful purpose connected with a function or activity of the controller; and

(b) the collection of the data is necessary for that purpose.

Subject to paragraph (1), where a controller collects personal data directly from a data subject, the controller shall, at the time of collecting the personal data, ensure that the data subject concerned is informed of:

(c) the identity and contact details of the controller;

(d) the purpose for which the data are being collected;

(e) the intended recipients of the data;

(f) whether or not the supply of the data by that data subject is voluntary or mandatory;

(g) the existence of the right to withdraw consent at any time,

without affecting the lawfulness of processing based on consent before its withdrawal;

(h) the existence of the right to request from the controller access to and rectification, restriction or erasure of personal data concerning the data subject or to object to the processing;

(i) the existence of automated decision making, including profiling, and information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;

(j) the period for which the personal data shall be stored;

(k) the right to lodge a complaint with the Authority;

(l) where applicable, that the controller intends to transfer personal data to another country and on the level of suitable protection afforded by that country; and

(m) any further information necessary to guarantee fair processing of the personal data, having regard to the specific circumstances in which the data are collected.

Where data are not collected directly from the data subject concerned, the controller or any person acting on his/her or its behalf shall ensure that the data subject is informed of the matters specified in paragraph (2).

However, a controller shall not be required to comply with paragraph (2) where:

(a) the data subject already has the information referred to in paragraphs (1) and (2); or

(b) the data are not collected from the data subject and:

(i) the provision of such information proves impossible

or would involve a disproportionate effort; or

(ii) the recording or disclosure of the data is laid down by law.

Article 40: Notification and reporting of personal data breach

In case of a personal data breach, the controller shall without undue delay, within 24 hours after having become aware of it, notify the personal data breach in a manner prescribed by the Authority in charge of data protection and privacy.

Where the controller fails to notify the personal data breach within the time limit specified in paragraph (1), he/she shall provide the Authority in charge of data protection and privacy with the reasons for the delay.

Where a processor becomes aware of a personal data breach, he/she shall notify the controller without any undue delay, within 24 hours after having become aware of it.

The reporting associated to the notification in paragraph (1) and (2) shall:

(a) describe the nature of the personal data breach, including where possible, the categories and approximate number of data subjects and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of any appropriate data protection officer or other contact point where more information may be obtained; and

(c) recommend measures to address the personal data breach, including, where appropriate, measures to

mitigate the possible adverse effects of the breach.

The controller shall specify the facts relating to the personal data breach, its effects and the remedial action taken so as to enable the Authority in charge of data protection and privacy to verify compliance with this article.

Article 41: Communication of personal data breach to data subject

Subject to article 39, where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, after notification the controller shall communicate the personal data breach to the data subject within 24 hours without undue delay.

The communication to the data subject shall describe in clear language, the nature of the personal data breach and set out the information and the recommendations provided for in article 39.

The communication of a personal data breach to the data subject shall not be required where:

(a) the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the breach, in particular, those that render the data unintelligible to any person who is not authorized to access it, such as encryption;

(b) the controller has taken subsequent measures to ensure that the high risk to the rights and freedoms of the data subject referred to in paragraph (1) is no longer likely to materialize; or

(c) the controller has made a public communication or similar measure whereby data subject is informed in an equally

effective manner.

Where the controller has not already communicated the personal data breach to the data subject, the Authority in charge of data protection and privacy shall, after having considered the likelihood of the personal data breach resulting in a high risk, require it to do so.

Article 42: Duty to destroy personal data

Where the purpose for keeping personal data has lapsed, every controller shall:

(a) destroy the data as soon as is reasonably practicable; and

(b) notify any processor holding the data.

Any processor who receives a notification under paragraph (1) (b) shall, as soon as is reasonably practicable, destroy the data specified by the controller.

Article 43: Lawful processing

Personal data shall be processed only when:

(a) the data subject consents to the processing for one or more specified purposes;

(b) the processing is necessary:

(i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;

(ii) for compliance with any legal obligation to which the controller is subject;

(iii) in order to protect the vital interests of the data

subject or another person;

(iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(v) the performance of any task carried out by a public entity;

(vi) the exercise, by any person in the public interest, of any other functions of a public nature;

(vii) for the legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or

(viii) for the purpose of historical, statistical or scientific research upon authorization by relevant institution.

Article 44: Security of processing

A data controller or data processor shall secure data in the possession or control of a data controller or data processor by adopting appropriate, reasonable, technical and organizational measures to prevent loss, damage, or unauthorized destruction and unlawful access to or unauthorized processing of data.

For the purposes of paragraph (1), the data controller shall take measures to:

a) identify reasonably foreseeable internal and external risks to data under that person's possession or control;

b) establish and maintain appropriate safeguards against risks;

c) regularly verify that the safeguards are effectively implemented; and

d) ensure that the safeguards are continually updated in response to new risks or deficiencies.

A data controller shall observe generally accepted information security frameworks, and specific industry or professional rules and regulations.

Article 45: Prior security check

Where the Authority in charge of data protection and privacy is of the opinion that the processing or transfer of data by a controller or processor may entail a specific risk to the privacy rights of data subjects, he/she may inspect and assess the security measures taken under article 44 prior to the beginning of the processing or transfer

The Authority in charge of data protection and privacy may carry out further inspection and assessment of the security measures under article 44.

CHAPTER VI: FREE FLOW OF NON-PERSONAL DATA

Article 46: Free movement of non-personal data

Non-personal data confinement shall be prohibited, unless they are justified on grounds of public security.

Any person shall immediately communicate to the Authority in charge of data protection and privacy any new or changes to an existing non-personal data confinement in accordance with the provisions of this Law.

Any person shall make the details of any non-personal data confinement, which he/she shall keep updated and provide its detailed changes to a single information point. The Authority in charge of data protection and privacy shall be informed of the address of their single information points.

The Authority in charge of data protection and privacy shall publish the link(s) of such point(s) on its website, along with a regularly updated consolidated list of all data confinement referred to in paragraph 3.

Article 47: Non-personal data availability for competent authorities

The provisions of this chapter shall not affect the mandate of competent authorities to request, or obtain, access to non-personal data for the performance of their official duties in accordance with applicable laws. Access to non-personal data by competent authorities may not be refused on the basis that the non-personal data are processed by another entity.

Where, after requesting access to non-personal data, a competent authority does not obtain access, that person may request assistance from

Authority in charge of data protection and privacy in accordance with the procedure set out in Article 49.

Article 48: Data portability

The Authority in charge of data protection and privacy shall encourage and facilitate the development of self-regulatory codes of conduct in order to contribute to a competitive data economy, based on the principles of transparency and interoperability and taking due account of open standards, covering, inter alia, the following aspects:

a) best practices for facilitating the switching of data processors and the data portability in a structured, commonly used and machine-readable format including open standard formats where required or requested by the data processor receiving the data;
b) minimum information requirements to ensure that users requesting integration are provided with sufficiently detailed, clear and transparent information regarding the processes and technical requirements. And this integration is done after a contract for data processing is concluded;
c) communication roadmaps taking a multi-disciplinary approach to raise awareness of the codes of conduct among relevant stakeholders.

Article 49: Single points of contact

Each entity shall designate an officer in charge of data protection which shall liaise with the single points of contact of other entities and the Authority in charge of data protection and privacy regarding the application of this chapter. Entities shall notify to the Authority in charge of data protection and privacy the designated officer in charge of data protection and any subsequent change thereto.

Where competent authority requests assistance from another entity, pursuant to Article 47 (2), in order to obtain access to data, it shall submit a duly justified request to the latter's designated officer in charge of data protection. The request shall include a written explanation of the reasons and the legal bases for seeking access to the data.

The officer in charge of data protection shall identify the relevant competent authority and transmit the request received pursuant to paragraph (2) to that competent authority.

Any information exchanged in the context of assistance requested and provided under Article 47 (2) shall be used only in respect of the matter for which it was requested.

The officer in charge of data protection shall provide users with general information on this chapter, including on the codes of conduct.

CHAPTER VII: PROCEDURES FOR DATA SHARING, TRANSFER, STORAGE AND RETENTION

Article 50: Obtaining access to personal data

Upon obtaining request from the data processor to access personal data, the data controller shall analyze the necessity of the processing and decide accordingly.

If the data controller rejects the request, he/she or it must specify the reasons for rejection.

Article 51: Eligibility to access personal data

Any person shall be eligible to access personal data, only if:

a. it is an entity incorporated in Rwanda, has known address and a valid certificate under Article 31;
b. he/she or it has a contract or a recommendation from the Government institution, any institution mentioned in (a) or holds a valid contract expressing the data subject's consent to process his/her personal data;
c. it is a public institution accessing for the public interest;
d. he/she or it presents documents that clearly demonstrate how the requested data are going to be used and the outcome of that processing.

Article 52: Remote access

Any data controller and/or data processor shall not remotely access the data from another country unless authorized by the Authority in charge of data protection and privacy.

Article 53: Regulation for personal data sharing or transfer in Rwanda

The Authority in charge of data protection and privacy shall put in place regulation and determine modalities for sharing and transferring of personal data in Rwanda.

Article 54: Transfer or sharing of personal data outside Rwanda

A data controller or data processor may transfer or share personal data to another country where:

(a) he/she or it has the authorization granted by the Authority in charge of data protection and privacy after providing proof of appropriate safeguards with respect to the protection of the personal data; and

(b) the data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer owing to the absence of appropriate safeguards;

(c) the transfer is necessary:

(i) for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;

(iii) for reasons of public interest as provided by law;

(iv) for the establishment, exercise or defense of a legal claim; or

(v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(vi) for the purpose of compelling legitimate interests pursued by the controller or the processor which are not overridden by the interests, rights and freedoms of the data subjects involved and where:

(A) the transfer is not repetitive and concerns a limited number of data subjects; and

(B) the controller or processor has assessed all the circumstances surrounding the data transfer operation and has, based on such assessment, provided to the Authority proof of appropriate safeguards with respect to the protection of the personal data; or

(d) the transfer is made from a register which, according to law, is intended to provide information to the public and which is open for consultation by the public or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down by law for consultation are fulfilled in the particular case.

A transfer pursuant to paragraph (1)(d) shall not involve the entirety of the personal data or entire categories of the personal data contained in the register and, where the register is intended for consultation by persons

having a legitimate interest, the transfer shall be made only at the request of those persons or in case they are to be the recipients.

Paragraph (1)(a) and (c)(i), (ii) and (vi) shall not apply to activities carried out by a public entity in the exercise of its functions.

The Authority in charge of data protection and privacy may request a person who transfers data to another country to demonstrate the effectiveness of the safeguards or the existence of compelling legitimate interests and may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as it may determine.

Article 55: Data hosting

Any controller and/or processor shall host and/or store the data in Rwanda.

Article 56: Data Embassy

The authority in charge of data protection and privacy shall determine modalities for operation and protection of data in the data embassy.

Article 57: Commercial use of personal data

Any person who intends to use personal data obtained pursuant to the provisions of this Law for commercial purposes, shall:

(a) seek and obtain express consent from a data subject; or
(b) be authorized by the law and the data subject has been informed of such use when collecting the data from the data subject.

A data controller or data processor that uses personal data for commercial purposes shall, where necessary, anonymize the data in such a manner as to ensure that the data subject is no longer identifiable.

The Authority in charge of data protection and privacy, shall prescribe detailed practice guidelines for commercial use of personal data in accordance with this Law.

Article 58: Migration and treatment of data after closure or change of business

The Authority in charge of data protection and privacy shall determine modalities for migration of data and decide the management of that data in the event of change or closure of business.

Article 59: Data Retention

A data controller or data processor shall retain data only as long as may be reasonably necessary to satisfy the purpose for which it is processed unless:

(a) the retention of the data is required or authorized by law;
(b) the retention of the data is necessary for a lawful purpose related to a function or activity for which the data is collected or processed;
(c) the retention of the data is required by a contract between the parties to the contract; or
(d) the data subject consents to the retention of personal data.

Where no retention period is required by the applicable law, personal data shall be retained for a period of ten (10) years and this period shall

provide the data subject with an opportunity to request access to personal data.

Paragraph (1) does not apply to data retained for:

(a) the prevention, detection, investigation, prosecution or punishment of an offence or breach of law;
(b) the national security purposes;
(c) the enforcement of a law which imposes a pecuniary penalty;
(d) the enforcement of legislation relating to public revenue collection;
(e) the conduct of proceedings before any court or tribunal; or
(f) historical, statistical, or research purposes; or
(g) any other retention as may be determined by the Authority in charge of data protection and privacy.

A data controller shall destroy or delete a record of personal data or de-identify the record at the expiry of the retention period.

The destruction or deletion of a record of personal data shall be done in a manner that prevents its reconstruction in an intelligible form.

The Authority in charge of data protection and privacy shall put in place other specific regulations for the retention period of personal data.

CHAPTER VIII: COMPLAINTS

Article 60: Complaints against breach and non-compliance.

Any person who believes that a data controller or data processor is infringing upon their rights or is in violation of this Law, may make a complaint in the prescribed manner to the Authority in charge of data protection and privacy.

A data controller or data processor may in writing make a complaint to the Authority in charge of data protection and privacy about any violation or non-compliance with this Law.

Article 61: Compensation

Any person who suffers damage by reason of a breach or non-compliance of this Law is entitled to compensation for that damage from the data controller or the data processor.

However, in the event where the damage resulted from circumstances that are beyond the control of the data controller, the right to seek compensation shall not apply.

Article 62: Authority to investigate complaints

The Authority in charge of data protection and privacy shall investigate every complaint made under this chapter and may direct a data controller or data processor to remedy any breach or take such action as the Authority in charge of data protection and privacy may specify to restore the integrity of data collected, processed or held by the data controller or data processor or the rights of the data subject.

<u>Article 63:</u> Appeals

Any person aggrieved by a decision of the Authority in charge of data protection and privacy under this Law shall appeal to the supervising Organ. The appeal shall be made within thirty (30) working days from the date of notice of the decision and a copy of the appeal shall be provided to the Authority in charge of data protection and privacy.

CHAPTER IX: MISCONDUCT, OFFENCES AND PENALTIES

Article 64: Administrative Sanctions

The Authority in charge of data protection and privacy may impose the administrative sanctions while respecting the principles of the rights to defense of all parties, transparency, impartiality and non-discriminatory procedures.

Article 65: Unlawful obtaining, processing or disclosing of data

Any natural person who unlawfully obtains, processes, discloses or procures the disclosure to another person of data held or processed by a data controller or data processor, commits an offence and is liable upon conviction to a fine not less than Five million (5.000.000) Rwandan Francs and not exceeding Ten million (10.000.000) Rwandan Francs or imprisonment not less than Six (6) months and not exceeding Two (2) years or both.

Article 66: Re-identification and processing of de-identified personal data

Any person who, knowingly or intentionally or recklessly:

(a) re-identifies personal data which has been de-identified by a data controller or a data processor, as the case may be; or

(b) re-identifies and processes such personal data as mentioned in clause (a)

without the consent of such data controller or data processor, then such person commits an offence and is liable upon conviction to a fine not less than Five million (5.000.000) Rwandan Francs and not exceeding Ten million (10.000.000) Rwandan Francs or imprisonment not less than

Two (2) years and not exceeding Five (5) years or both.

Article 67: Unlawful destruction, deletion, concealment or alteration of data

Any natural person who unlawfully destroys, deletes, misleads, conceals or alters data, commits an offence and is liable upon conviction to a fine not less than Five million (5.000.000) Rwandan Francs and not exceeding Ten million (10.000.000) Rwandan Francs or imprisonment not less than Six (6) months and not exceeding Two (2) years or both.

Article 68: Unlawful sale of data

Any natural person who unlawfully sells or offer for sale data, commits an offence and is liable upon conviction to a fine not less than Five million (5.000.000) Rwandan Francs and not exceeding Ten million (10.000.000) Rwandan Francs or imprisonment not less than Two (2) years and not exceeding Five (5) years or both.

Article 69: Unlawful collecting or processing of sensitive personal data

Any natural person who unlawfully collects and/or processes sensitive personal data commits an offence. Upon conviction, is liable to a fine not less than Five million (5.000.000) Rwandan Francs and not exceeding Ten million (10.000.000) Rwandan Francs or imprisonment not less than Two (2) years and not exceeding Five (5) years or both.

Article 70: Providing false information

Any controller or processor who knowingly provides false or misleading information during registration commits an offence. Upon conviction, is liable to a fine not less than Five hundred thousand (500.000) Rwandan Francs and not exceeding One million (1.000.000) Rwandan Francs or imprisonment not less than One (1) year and not exceeding Three (3) years or both.

Article 71: Offences by corporations

Where an offence under this chapter is committed by a corporate entity, the corporate entity knowingly and intentionally authorizes or permits the contravention commits an offence.

Upon conviction, the court may order the corporation to pay a fine of 5 % of the annual turnover.

Article 72: Additional penalties

Except penalties provided for under this Law, the court may, in all cases, order the confiscation of property and belongings used in the omission of any of the offences provided for in this Law and the proceeds gained.

The court may also, permanently or temporary for the period that it considers appropriate, order the closure of the premise or corporate body in which any of the offences provided for in this Law has been committed, if the offence was committed.

CHAPTER X: MISCELLANEOUS AND FINAL PROVISIONS

Article 73: Regulations

Without prejudice to the provisions of this law, competent authorities shall put in place regulations related to personal data protection and privacy within sectors under their mandate.

Article 74: Transitional period

With regards to administrative requirements, the existing data controllers and data processors must comply with the provisions of this Law within one (1) year as from its publication in the Official Gazette of the Republic of Rwanda.

Article 75: Drafting, consideration and adoption of this Law

This law was drafted in English, considered and adopted in Kinyarwanda.

Article 76: Repealing provision

All prior legal provisions contrary to this Law are repealed.

Article 77: Commencement

This Law comes into force on the date of its publication in the Official Gazette of the Republic of Rwanda.