



0
Special of
21

60^{ème} Année
Journal Officiel n° Spécia
15/10/2021

aire

page/urup

reho bwite by'umuntu

l privacy

e personnel et de la vie privée

**LAW N° 058/2021 OF 13/10/2021
RELATING TO THE PROTECTION OF
PERSONAL DATA AND PRIVACY**

TABLE OF CONTENTS

**CHAPTER ONE: GENERAL
PROVISIONS**

Article One: Purpose of this Law

Article 2: Scope of this Law

Article 3: Definitions

**CHAPTER II: PROCESSING AND
QUALITY OF PERSONAL DATA**

Section One: Processing of personal data

**Article 4: Authorisation to process personal
data**

Article 5: Privacy of the data subject

Article 6: Consent of the data subject

Article 7: Indication of other matters in the declaration of consent

Article 8: Right of the data subject to withdraw his or her consent

Article 9: Processing a child's personal data

Article 10: Grounds for processing sensitive personal data

Article 11: Safeguards to process sensitive personal data

Article 12: Processing personal data of a convict

Article 13: Processing of personal data which does not require data subject's identification

Article 14: Source of personal data

Section 2: Quality of personal data and records of personal data

Article 15: Quality of personal data

Article 16: Personal data logging

Article 17: Maintaining records of processed personal data

CHAPTER III: RIGHTS OF THE DATA SUBJECT

Article 18: Right to personal data

Article 19: Right to object

Article 20: Right to personal data portability

Article 21: Right not to be subject to a decision based on automated data processing

Article 22: Right to restriction of processing of personal data

Article 23: Right to erasure of personal data

Article 24: Right to rectification

Article 25: Right to designate an heir to personal data

Article 26: Right to representation

CHAPTER VI: TASKS AND POWERS OF THE SUPERVISORY AUTHORITY IN MATTERS RELATING TO THE PROTECTION OF PERSONAL DATA AND PRIVACY

Article 27: Duties of the supervisory authority in matters relating to the protection of personal data and privacy

Article 28: Powers of the supervisory authority in matters relating to the protection of personal data and privacy

CHAPTER V: REGISTRATION OF A DATA CONTROLLER AND A DATA PROCESSOR

Article 29: Registration as a data controller or a data processor

Article 30: Requirements for registration as

a data controller or a data processor

Article 31: Issuance of a registration certificate

Article 32: Reporting a change after receiving a registration certificate

Article 33: Renewal of a registration certificate

Article 34: Modification of a registration certificate

Article 35: Cancellation of a registration certificate

Article 36: Register of data controllers and data processors

CHAPTER VI: OBLIGATIONS OF THE DATA CONTROLLER AND THE DATA PROCESSOR

Article 37: Principles relating to processing of personal data

Article 38: Duties of the data controller and the data processor

Article 39: Designation of a representative of the data controller or the data processor

Article 40: Designation of the personal data protection officer

Article 41: Duties of the personal data protection officer

Article 42: Information to be provided during personal data collection

Article 43: Notification of personal data breach

Article 44: Report on personal data breach

Article 45: Communication of a personal data breach to the data subject

Article 46: Lawful processing of personal data

Article 47: Measures to ensure security of personal data

CHAPTER VII: SHARING, TRANSFER, STORAGE AND RETENTION OF PERSONAL DATA

Article 48: Sharing and transfer of personal data outside Rwanda

Article 49: Contract for transfer of personal data

Article 50: Storage of personal data

Article 51: Migration and management of personal data after change or closure of business

Article 52: Retention of personal data

CHAPTER VIII: MISCONDUCTS, OFFENCES AND SANCTIONS

Section One: Administrative misconducts and sanctions

Article 53: Administrative misconducts

Article 54: Filing an application to the court

Article 55: Place where the administrative fine is deposited

Section 2: Offences and penalties

Article 56: Accessing, collecting, using, offering, sharing, transfer or disclosing of personal data in a way that is contrary to this Law

Article 57: Re-identification of de-identified personal data in a way that is contrary to this Law

Article 58: Destruction, erasure, concealment or alteration of personal data in a way that is contrary to this Law

Article 59: Sale of personal data in a way that is contrary to this Law

Article 60: Collecting or processing of sensitive personal data in a way that is contrary to this Law

Article 61: Providing false information

Article 62: Punishment of a corporate body or a legal entity

Article 63: Additional penalties

**CHAPTER IX: MISCELLANEOUS
TRANSITIONAL AND FINAL
PROVISIONS**

**Article 64: Organ in charge of settlement of
disputes**

Article 65: Right to claim for compensation

Article 66: Power to put in place regulations

Article 67: Transitional period

**Article 68: Drafting, consideration and
adoption of this Law**

Article 69: Repealing provision

Article 70: Commencement

**LAW N° 058/2021 OF 13/10/2021
RELATING TO THE PROTECTION OF
PERSONAL DATA 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 sitting of
12 August 2021;

Pursuant to the Constitution of the Republic of
Rwanda of 2003 revised in 2015, especially in
Articles 23, 64, 69, 70, 88, 90, 91, 93, 106,
120, 122 and 176;

Pursuant to the African Union Convention on
cyber security and personal data protection
adopted in Malabo, Equatorial Guinea, on
27 June 2014, ratified by Presidential Order

n° 104/01 of 18/09/2019;

ADOPTS:

CHAPTER ONE: GENERAL
PROVISIONS

Article One: Purpose of this Law

This Law aims at the protection of personal data and privacy and determines their processing.

Article 2: Scope of this Law

This Law applies to:

- 1° the processing of personal data by electronic or other means using personal data through an automated or non automated platform;
 - 2° the data controller, the data processor or a third party who:
 - a) is established or resides in Rwanda
-

and processes personal data while in Rwanda;

- b) is neither established nor resides in Rwanda, but processes personal data of data subjects located in Rwanda.

Article 3: Definitions

In this Law, the following terms have the following meanings:

1° **personal data:** any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person;

2° **sensitive personal data:** information revealing a person's race, health status, criminal records, medical records, social origin, religious or philosophical beliefs, political opinion, genetic or biometric information, sexual life or

family details;

3° **encryption:** technical method used to render the content of data unreadable to any person who is not authorised to access it;

4° **processing of personal data:** an 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 access to, obtaining, collection, recording, structuring, storage, adaptation or alteration, retrieval, reconstruction, concealment, consultation, use, disclosure by transmission, sharing, transfer, or otherwise making available, sale, restriction, erasure or destruction;

5° **register of data controllers and data processors:** a system of records, physical or electronic of registered data controllers and data processors;

- 6° **privacy:** a fundamental right of a person to decide who can access his or her personal data, when, where, why and how his or her personal data can be accessed;
- 7° **significant consequences:** effects that are as similarly significant in their impact as legal effects and that adversely affect a data subject's behaviour or choices;
- 8° **legal consequences:** effects that adversely affect a person's legal status or his/her legal rights;
- 9° **tokenisation:** the process of replacing sensitive data with unique identification symbols that retain all the essential information about the data without compromising its security;
- 10° **vital interests:** interests linked to life or death of data subject;
- 11° **profiling:** form of automated
-

processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse and predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

12° **personal data logging:** the process of recording personal data processing activities over a period of time for the purpose of event monitoring and auditing in an automated processing system;

13° **personal data breach:** a breach of personal data security leading to unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

14° **pseudonymisation:** 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 kept separately;

15° **data subject:** a natural person from whom or in respect of whom, personal data has been requested and processed;

16° **recipient:** a natural person, a public or private corporate body or legal entity to which the personal data are disclosed;

17° **user:** a natural person, a public or private corporate body or a legal entity, who uses or who requests personal data processing service;

18° **consent of the data subject:** freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by an oral, written or electronic statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

19° **data controller:** natural person, public or private corporate body or legal entity which, alone or jointly with others, processes personal data and determines

the means of their processing;

20° **person:** natural person, corporate body or legal entity;

21° **third party:** natural person, corporate body or legal entity other than the data subject, the data controller, the data processor and persons who, under the authority of the data controller, are authorised to process personal data;

22° **competent authority:** sectoral authority responsible for overseeing sector-specific compliance in conjunction with the supervisory authority;

23° **supervisory authority:** a public authority in charge of cyber security;

24° **data processor:** natural person, public or private corporate body or legal entity which is authorised to process personal data on behalf of the data controller.

CHAPTER II: PROCESSING AND QUALITY OF PERSONAL DATA

Section One: Processing of personal data

Article 4: Authorisation to process personal data

The processing of personal data carried out by the data processor is governed by a written contract between the data processor and the data controller.

The data processor processes personal data on behalf of the data controller subject to a written contract referred to in Paragraph One of this Article.

The data controller authorises the data processor who provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing meets the requirements of this Law.

Article 5: Privacy of the data subject

The data controller, the data processor or a third

party processes personal data in a manner which does not infringe on the privacy of the data subject.

Article 6: Consent of the data subject

Where the processing of personal data is based on the consent of the data subject, data subject demonstrates that he or she has consented to the processing of his or her personal data for a specified purpose.

The consent of the data subject is valid only when it is based on the data subject's free decision after being informed of the consequences of his or her consent.

The consent of the data subject may be made in oral, written or electronic form.

Article 7: Indication of other matters in the declaration of consent

The data subject's declaration of consent that contains other matters must clearly indicate those other matters to which he or she consents in one of the official languages that is understandable to him or her.

Any part of the declaration referred to in Paragraph One of this Article which constitutes an infringement of the provisions of this Law cannot be binding.

Article 8: Right of the data subject to withdraw his or her consent

The data subject has the right to withdraw his or her consent at any time.

The withdrawal of consent by the data subject does not affect the lawfulness of processing of personal data based on consent before its withdrawal.

The withdrawal of consent by the data subject is as easy as expressing it.

The withdrawal of consent by the data subject takes effect as of the date on which the data subject applied for it.

Article 9: Processing a child's personal data

Where the data controller, the data processor or a third party knows that personal data

belong to a child under the age of sixteen (16) years, he or she must obtain the consent of a holder of parental responsibility over the child in accordance with relevant Laws.

Subject to the provisions of other Laws, the consent obtained on behalf of the child is acceptable only if it is given in the interest of the child.

However, the consent is not required to process the child's personal data if it is necessary for protecting the vital interest of the child.

Article 10: Grounds for processing sensitive personal data

The data controller or the data processor processes sensitive personal data only if:

- 1° the processing is based on the data subject's consent;
 - 2° the processing is necessary for the purposes of carrying out the obligations of the data controller, of the data processor or exercising specific rights of the data subject in accordance with relevant Laws;
-

- 3° the processing is necessary to protect the vital interests of the data subject or of any other person;
- 4° the 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;
- 5° the processing is necessary for archiving purposes in the public interest or scientific and historical research purposes or statistical purposes.

Article 11: Safeguards to process sensitive personal data

When processing sensitive personal data, the data controller or the data processor must:

- 1° comply with requirements for personal data protection or personal data monitoring as required by this Law;
-

- 2° comply with applicable sensitive personal data retention periods established by this Law;
- 3° put in place measures to strengthen capacities of staff involved in the processing of sensitive personal data;
- 4° put in place measures to access sensitive personal data processed by the data controller or the data processor;
- 5° implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed to the data subject, including, where appropriate, storing sensitive personal data separately from other types of data, and applying measures such as tokenisation, pseudonymisation or encryption.

Article 12: Processing personal data of a convict

Processing personal data of a convict is carried

out under the supervision of the supervisory authority in accordance with the provisions of this Law.

The data controller or the data processor puts in place appropriate safeguards to ensure the respect of rights and freedoms of the data subject.

Article 13: Processing of personal data which does not require data subject's identification

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

In case the data controller or the data processor is unable to identify the data subject because of the alteration of his or her personal data, the data controller informs the data subject in writing or electronically, if necessary.

However, the data subject, with respect to his or her rights, provides additional information

enabling his or her identification.

Article 14: Source of personal data

The data controller or the data processor requests personal data directly from the data subject.

However, a person can collect personal data from another person, another source or a public institution if:

- 1° the personal data is open to the public;
- 2° the data subject has deliberately made the personal data public;
- 3° the data subject has consented to the collection of personal data from another source;
- 4° the collection of the personal data from another source complies with the provisions of this Law.

Section 2: Quality of personal data and records of personal data

Article 15: Quality of personal data

The data controller or the data processor ensures that the personal data is complete, accurate, kept up to date and not misleading having regard to the purposes for which they are processed.

Article 16: Personal data logging

The data controller or the data processor ensures personal data logging at least on the following data operations:

- 1° data collected;
- 2° data altered;
- 3° data accessed;

- 4° data disclosed including data sharing and transfer;
- 5° combined data;
- 6° erased data.

Personal data logging must indicate justification, date and time of such operation and, where possible, the contact details of the person who accessed or disclosed the personal data.

data, as well as the contact details of the recipients of the data.

The supervisory authority may require the data controller or the data processor to provide access to the personal data logging so as to verify the lawfulness of the personal data processing.

Article 17: Maintaining records of processed personal data

The data controller or the data processor must maintain a record of all personal data processing activities under his or her responsibility that indicates:

- 1° the name and contact details of the data controller and, where applicable, the data processor, the controller's representative or the data protection officer;
 - 2° the purposes of the processing of personal data;
 - 3° a description of the categories of data subjects and of the categories of personal data;
-

- 4° a full list of the recipients to whom personal data have been or will be disclosed, including those based in other countries;
- 5° a description of transfers of personal data to any country outside Rwanda;
- 6° where possible, the envisaged data retention periods for the different categories of personal data.

The data controller or the data processor submits the records of personal data processing activities to the supervisory authority on request.

CHAPTER III: RIGHTS OF THE DATA SUBJECT

Article 18: Right to personal data

Without prejudice to other relevant Laws, the data subject may, in writing or electronically, request from the data controller or the data processor the following:

- 1° to provide him or her with the information relating to the purposes of the processing of personal data;
- 2° to provide him or her with a copy of personal data;
- 3° to provide him or her with a description of personal data that the data controller or the data processor holds, including data on the contact details of a third party or the categories of third parties who have or had access to personal data;
- 4° to inform him or her of the source of the personal data in case his or her personal data have not been obtained from the data subject;
- 5° to inform him or her in case his or her personal data have been transferred to a third country or to an international organisation.

The right referred to in Item 2° of Paragraph One of this Article is not exercised if:

- 1° it may adversely affect the rights and freedoms of other persons;
 - 2° legal professional privilege or another
-

legal obligation of confidentiality applies;

3° the data relates to information management or information about the data subject or relates to ongoing negotiations with the data subject requester;

4° the data relates to the data subject's confidential references, examination scripts or examination marks.

The data controller or the data processor must provide the data subject with his or her personal data in a clear and concise manner.

The data subject who is not satisfied with the response of the data controller or the data processor may appeal to the supervisory authority within thirty (30) days from the date of receipt of the response.

If the data subject appeals, the supervisory authority responds to his or her appeal within sixty (60) days from the date of receipt of the appeal.

Article 19: Right to object

The data subject, at any time in writing or electronically, may request the data controller or the data processor to stop processing his or her personal data which causes or is likely to cause loss, sadness or anxiety to the data subject.

However, this right does not apply if the data controller or the data processor demonstrates compelling legitimate grounds for the personnel data processing, which override the interests, rights and freedoms of the data subject or for the establishment of the legal claim.

The data subject, at any time in writing or electronically, may request the data controller or the data processor to stop processing personal data of the data subject if personal data are processed for direct marketing purposes, including profiling to the extent that it is related to such direct marketing.

The data controller or the data processor, within thirty (30) days from the date of receipt of the request, must inform the concerned data subject in writing or electronically of the

compliance with the request or reasons for non-compliance.

The data subject who is not satisfied with the response of the data controller or the data processor may appeal to the supervisory authority within thirty (30) days from the date of receipt of the response.

If the data subject appeals, the supervisory authority responds to his or her appeal within sixty (60) days from the date of receipt of the appeal.

Article 20: Right to personal data portability

The data subject has the right to request the data controller in writing or electronically to resend the personal data concerning him or her as it was provided to the data controller, in a structured and readable format.

The data subject also has the right to request the data controller in writing or electronically to have his or her personal data transmitted to another data controller, where technically feasible, without hindrance.

The data controller, within thirty (30) days from the date of receipt of the request, must inform the concerned data subject in writing or electronically of personal data portability.

The data subject who is not satisfied with the response of the data controller may appeal to the supervisory authority within thirty (30) days from the date of receipt of the response.

If the data subject appeals, the supervisory authority responds to his or her appeal within sixty (60) days from the date of receipt of the appeal.

Article 21: Right not to be subject to a decision based on automated data processing

The data subject has the right not to be subject to a decision based solely on automated personal data processing, including profiling, which may produce legal consequences or significant consequences to him or her.

However, the provisions of Paragraph One of this Article do not apply if the decision:

- 1° is based on the data subject's explicit consent;
- 2° is necessary for entering into, or performance of, a contract between the data subject and the data controller;
- 3° is authorised by Laws to which the data controller is subject and also puts in place suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

Any automated processing of personal data intended to evaluate certain personal aspects relating to a natural person does not base on sensitive personal data unless one of the grounds set out in Article 10 of this Law is met.

Article 22: Right to restriction of processing of personal data

The data subject or the supervisory authority has the right to restrict the data controller from processing personal data for a given period if:

- 1° the accuracy of personal data is
-

contested by the data subject, pending the verification of their accuracy;

- 2° the processing is unlawful and the data subject requests the erasure of the personal data or the restriction of the use of some of them;
- 3° the data subject has objected to the processing of personal data pending the verification whether the legitimate grounds of the controller override those of the data subject.

The right to restriction of processing of personal data described in Paragraph One of this Article is not exercised if the processing of personal data:

- 1° is necessary for the protection of the rights of another person;
- 2° is necessary for reasons of public interest.

The data controller must, before lifting the restriction of processing of personal data referred to in item 1° of Paragraph 2 of this

Article, inform the data subject in writing or electronically.

Article 23: Right to erasure of personal data

The data subject has the right to request the data controller in writing or electronically for erasure of his or her personal data where:

- 1° the personal data are no longer necessary in relation to the purposes for which they were collected or processed;
- 2° the data subject withdraws consent on which the personal data processing is based and where there is no other legal ground for the processing;
- 3° the data subject objects to the processing of personal data and there are no overriding legitimate grounds for the processing;
- 4° the personal data have been unlawfully processed.

The data controller who has disclosed personal

data to a third party or has posted the personal data in the public domain must, in writing or electronically, inform a third party processing such data that the data subject has requested the erasure of any links to, or copy of, those personal data.

However, the right to request the erasure of personal data does not apply to the extent that processing is necessary:

- 1° for reasons of public interest;
- 2° for historical or scientific research purposes or statistical purposes;
- 3° for compliance with a legal obligation 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 data controller;
- 4° for the establishment, exercise or defence of legal claims in the interest of the data controller.

The data controller, within thirty (30) days from the date of receipt of the request, must inform the concerned data subject in writing or

electronically of the erasure of his or her personal data.

The data subject who is not satisfied with the response of the data controller may appeal to the supervisory authority within thirty (30) days from the date of receipt of the response.

If the data subject appeals, the supervisory authority responds to his or her appeal within sixty (60) days from the date of receipt of the appeal.

Article 24: Right to rectification

The data subject has the right to request the data controller the rectification of his or her personal data.

The data subject has the right to have incomplete personal data completed, where necessary.

The data controller, within thirty (30) days from the date of receipt of the request, must inform the data subject in writing or electronically of the rectification of his or her personal data.

The data subject who is not satisfied with the response of the data controller may appeal to the supervisory authority within thirty (30) days from the date of receipt of the response.

If the data subject appeals, the supervisory authority responds to his or her appeal within sixty (60) days from the date of receipt of the appeal.

Article 25: Right to designate an heir to personal data

The personal data of the data subject are not subject to succession.

However, where the data subject had left a will, the data subject provides his or her heir with full or restricted rights relating to the processing of personal data kept by the data controller or the data processor, if such personal data still need to be used.

Article 26: Right to representation

The right of the data subject to representation is exercised where:

- 1° the data subject is under sixteen (16) years of age, in which case he or she is represented by a person who has parental authority over him or her or who was appointed as his or her guardian;
- 2° the data subject has a physical impairment and is unable to represent himself or herself, in which case he or she is represented by his or her parent, adopter, a centre or an association that caters for him or her guardian appointed by a court;
- 3° the data subject has a medically determinable mental impairment and is unable to represent himself or herself, in which case he or she is represented by his or her parent, adopter, a centre or an association that caters for him or her or the guardian appointed by a court;
- 4° there is any other reason, in which case he or she is represented by another person authorised in writing by the data subject in accordance with relevant law.

**CHAPTER IV: DUTIES AND POWERS
OF THE SUPERVISORY AUTHORITY
IN MATTERS RELATING TO THE
PROTECTION OF PERSONAL DATA
AND PRIVACY**

**Article 27: Duties of the supervisory
authority in matters relating to the
protection of personal data and privacy**

The supervisory authority has the following
duties:

- 1° to oversee the implementation of this
law;
 - 2° to respond to every legitimate request
for an opinion regarding personal data
processing;
 - 3° to inform the data subject, the data
controller, the data processor and a third
party of their rights and obligations;
 - 4° to put in place a register of data
controllers and data processors;
 - 5° to investigate the subject matter of the
-

complaint lodged by the data subject or the data controller, the data processor or a third party relating to the processing of personal data and inform them of the outcome of the investigation within a reasonable period;

6° to receive and consider the data subject's appeal;

7° to advise on matters relating to the protection of personal data and privacy;

8° cooperate with authorities, organisations or entities operating within the country or abroad in the protection of personal data and privacy.

Article 28: Powers of the supervisory authority in matters relating to the protection of personal data and privacy

The supervisory authority has powers to:

1° to issue registration certificate as provided for by this Law;

2° ensure that the processing of personal data is consistent with the provisions of

this Law;

- 3° ensure that information and communication technologies do not constitute a threat to public freedom and the privacy of a person;
- 4° to put in place a regulation relating to the application of this Law;
- 5° to impose administrative sanctions in accordance with the provisions of this Law.

CHAPTER V: REGISTRATION OF THE DATA CONTROLLER AND THE DATA PROCESSOR

Article 29: Registration as a data controller or a data processor

A person who intends to be a data controller or a data processor must register with the supervisory authority.

Article 30: Requirements for registration as a data controller or a data processor

An applicant for registration as a data controller

or a data processor must indicate the following

- 1° his or her identity and his or her designated single point of contact;
 - 2° the identity and address of his or her representative if he or she has nominated any;
 - 3° a description of personal data to be processed and the category of data subjects;
 - 4° whether or not the applicant holds or is likely to hold the types of personal data based on the sectors in which it operates;
 - 5° the purposes of the processing of personal data;
 - 6° the categories of recipients to whom the data controller or the data processor intends to disclose the personal data;
 - 7° the country to which the applicant intends to directly or indirectly transfer the personal data;
-

8° risks in the processing of personal data and measures to prevent such risks and protect personal data.

The supervisory authority may put in place a regulation determining additional requirements to be met by an applicant for registration as a data controller or a data processor.

Article 31: Issuance of a registration certificate

The supervisory authority issues a registration certificate to an applicant for registration as a data controller or a data processor who meets the requirements for registration within thirty (30) working days from the date of reception of the registration application.

The supervisory authority puts in place a regulation determining the period of validity of the registration certificate.

Article 32: Reporting a change after receiving a registration certificate

After receiving a registration certificate, if

There is a change in the grounds on which a registration certificate was issued, the data controller or the data processor who received it notifies the supervisory authority in writing or electronically within fifteen (15) working days from the date on which such a change occurred.

The supervisory authority, as soon as it is informed of change referred to under Paragraph One of this Article and gives its satisfaction, updates the information.

Article 33: Renewal of a registration certificate

The data controller or the data processor who holds a registration certificate may apply for its renewal within forty-five (45) working days before the expiry date of the existing certificate.

The supervisory authority responds in writing or electronically to the application referred to under Paragraph One of this Article, within thirty (30) working days following receipt of the application.

The supervisory authority puts in place a

regulation determining requirements for renewal of the registration certificate.

Article 34: Modification of a registration certificate

The supervisory authority, on its own motion or on request by the registration certificate holder, may modify the registration certificate before its expiry, if the supervisory authority believes that modification is needed to respond on:

- 1° change that occurred on applicable laws;
- 2° a change in the information that he or she provided that may affect the registration certificate.

Article 35: Cancellation of a registration certificate

The supervisory authority may cancel the registration certificate before its date of expiry if the registration certificate holder:

- 1° has submitted false or misleading information;
- 2° fails to comply with requirements of this

Law or terms and conditions specified in the certificate.

Before cancellation of the registration certificate, the supervisory authority provides the certificate holder with fifteen (15) working days prior notice in writing or electronically, requesting for explanations on non-compliance with the provisions of Paragraph One of this Article.

Article 36: Register of data controllers and data processors

The supervisory authority puts in place a register of data controllers and data processors. Such a register is kept and managed by the supervisory authority, which also determines its form and the manner in which it is used.

The supervisory authority may, at the request of the data controller or the data processor who has an outdated entry in the register of data controllers and data processors, erase the entry from the register.

The supervisory authority puts in place a regulation determining modalities under which persons with justified reasons may have the

right of access to the register of data controllers and data processors for consultation, or to be issued with a certified copy or an extract of any entry in such a register.

CHAPTER VI: OBLIGATIONS OF THE DATA CONTROLLER AND THE DATA PROCESSOR

Article 37: Principles relating to processing of personal data

The data controller and the data processor ensure that the data subject's personal data:

- 1° are processed lawfully, fairly and in a transparent manner;
 - 2° are collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
 - 3° are related to the purposes for which their processing was requested;
 - 4° are 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;

5° are 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;

6° are processed in compliance with the rights of data subjects.

Article 38: Duties of the data controller and the data processor

In compliance with the principles of the processing of personal data, the data controller and the data processor discharge the following duties:

1° to implement appropriate technical and organisational measures;

2° to keep a record of personal data processing operations;

3° to carry out personal data protection impact assessments where the processing of personal data is likely to result in a high risk to the rights and freedoms of a natural person;

4° to perform such other duty as may be assigned to him or her by the supervisory authority.

The personal data protection impact assessment referred to in item 3° of Paragraph one of this Article is carried out in case of:

- 1° a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing of personal data, including profiling, and on which decisions that produce effects concerning such persons are based;
- 2° processing on a large scale of sensitive personal data;
- 3° a systematic monitoring of a publicly accessible area on a large scale;
- 4° processing of personal data identified by the supervisory authority as likely to result in a high risk to the rights and freedoms of natural persons;

5° new technologies used to process personal data.

Article 39: Designation of a representative of the data controller or data processor

The data controller or the data processor who is neither established nor resides in Rwanda, but processes personal data of data subjects located in Rwanda, designates in writing a representative in Rwanda to comply with his or her obligations under this Law.

The supervisory authority puts in place a regulation governing the designation of a representative of the data controller or data processor.

Article 40: Designation of the personal data protection officer

The data controller and the data processor designate a data protection officer where:

- 1° the processing of personal data is carried out by public or private corporate body or a legal entity, except courts;

- 2° the core activities of the data controller or the data processor consist of personal data processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale;
- 3° the core activities of the data controller or the data processor consist of processing on a large scale of special categories of data pursuant to Article 10 of this Law and personal data relating to criminal convictions referred to in Article 12 of this Law.

A group of undertakings may appoint a single personal data protection officer provided that the data protection officer is easily accessible from each establishment.

Where the data controller or the data processor is a public authority or body, a single personal data protection officer may be designated for several such authorities or bodies, taking account of their organizational structure and size.

In cases other than those referred to in Paragraph one of this Article, the data controller or the data processor or associations and other bodies representing categories of data controllers or data processors may designate a personal data protection officer in accordance with the provisions of this Law.

The data protection officer is designated on the basis of professional qualities, experience and knowledge of personal data protection practices and the ability to fulfil the tasks assigned to him or her.

The personal data protection officer may be a permanent staff member of the data controller or the data processor, or a person who fulfils the tasks on the basis of a service contract.

The data controller or the data processor must publish the contact details of the personal data protection officer and communicate them to the supervisory authority.

Article 41: Duties of the personal data protection officer

The personal data protection officer has the following duties:

- 1° to inform and advise the data controller, the data processor and the employees who carry out personal data processing of their obligations pursuant to this Law;
 - 2° to monitor, in his or her area of work, compliance with this Law and with the policies of the data controller or data processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in personal data processing operations, and the related audits;
 - 3° to provide advice where requested as regards the data protection impact assessment and monitor its performance;
 - 4° to cooperate with the supervisory authority and to act as its contact point on issues relating to processing of personal data, including the prior consultation with the supervisory authority, and to consult, where appropriate, with regard to any other matter.
-

The personal data protection officer must in the performance of his or her tasks have due regard to the risk associated with personal data processing operations, considering the nature, scope, context and purpose of processing.

Article 42: Information to be provided during personal data collection

The data controller collects personal data for a lawful purpose connected to the activity of the data controller and when the data is necessary for that purpose.

The data controller who collects personal data informs the data subject of the following:

- 1° his or her identity and contact details;
 - 2° the purposes for which personal data are collected;
 - 3° recipients of such personal data;
 - 4° whether the data subject has the right to provide personal data voluntarily or mandatorily;
-

- 5° the existence of the right to withdraw consent at any time and that such withdrawal does not affect the lawfulness of the processing of personal data based on consent before its withdrawal;
 - 6° the existence of the right to request from the data controller access and rectification, restriction or erasure of personal data concerning the data subject or to object to the processing of the data;
 - 7° 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 personal data for the data subject;
 - 8° the period for which personal data will be stored;
 - 9° the right to appeal to the supervisory authority;
 - 10° where applicable, that he or she can transfer personal data outside Rwanda and he or she assures him or her of their security;
-

11° any further information likely to guarantee fair processing of the personal data, having regard to the specific circumstances in which the data are collected.

However, the data controller is not required to comply with the provisions of Paragraph 2 of this Article if:

- 1° the data subject already has the information referred to in Paragraph One of this Article;
- 2° the provision of such information proves impossible or involves a disproportionate effort;
- 3° the recording or disclosure of the personal data is provided for by the Law

Article 43: Notification of personal data breach

In case of personal data breach, the data controller, within forty-eight (48) hours after being aware of the incident, must communicate the personal data breach to the supervisory authority.

Where the data processor becomes aware of a personal data breach, he or she notifies the data controller within forty-eight (48) hours after becoming aware of the incident.

Article 44: Report on personal data breach

The data controller draws up a report on a personal data breach and submits it to the supervisory authority not later than seventy-two (72) hours, with all facts available.

The report describes at least:

- 1° the nature of the personal data breach, including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - 2° the contact details of the personal data protection officer or other contact point where more information can be obtained;
 - 3° the measures taken to address the personal data breach, including measures to mitigate its possible
-

adverse effects;

- 4° the acts relating to personal data breaches, the consequences of the personal data breach and the measures taken to rectify such a breach;
- 5° his or her proposal for communicating the personal data breach to affected data subjects and the timeline for such a communication, for approval by the supervisory authority.

Article 45: Communication of a personal data breach to the data subject

Where the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject, the data controller communicates the personal data breach to the data subject in writing or electronically, after having become aware of it.

However, the data controller is not required to communicate the personal data breach to the data subject if:

- 1° the data controller has implemented
-

appropriate technical and organisational protection measures in relation to personal data breached such that the personal data breach is unlikely to result in a high risk to the rights and freedoms of the data subject;

- 2° the data controller has taken measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialize;
- 3° the data controller communicated it to the public whereby the data subject is informed in an equally effective manner.

If the data controller has not communicated the personal data breach to the data subject, and the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject, the supervisory authority may request the data controller to communicate the personal data breach to the data subject in writing or electronically.

Article 46: Lawful processing of personal data

The data controller or the data processor lawfully processes personal data if:

- 1° the data subject has given consent to the processing of his or her personal data for purposes explained to him or her;
 - 2° processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
 - 3° the data controller executes a legal obligation to which he or she is a subject;
 - 4° it is necessary for protection of vital interests of the data subject or any other person;
 - 5° it is necessary for the performance of a duty carried out in the public interest or in the exercise of official authority vested in the data controller;
 - 6° it is carried out for the performance of
-

duties of a public entity;

- 7° it is intended for legitimate interests pursued by the data controller or by a third party to whom the personal data are disclosed, unless the processing of personal data is unwarranted in any particular case having regard to the prejudice to the rights and freedoms or legitimate interests pursued by the data subject;
- 8° it is carried out for research purposes upon authorisation by relevant institution.

Article 47: Measures to ensure security of personal data

The data controller or the data processor must ensure security of the personal data in his or her possession by, adopting appropriate, reasonable technical measures to prevent loss, damage or destruction of personal data.

For purposes of enforcing the provisions of Paragraph One of this Article, the data controller or the data processor takes the following measures to ensure security of personal data:

- 1° identify foreseeable risks to personal data under that person's possession or control, establish and maintain appropriate safeguards against those risks;
- 2° regularly verify whether the personal data security safeguards are effectively implemented;
- 3° ensure that the personal data security safeguards are continually updated in response to new risks or any identified deficiencies.

When the supervisory authority is of the opinion that processing or transferring personal data may infringe the rights and privacy of the data subject, the supervisory authority conducts an inspection and assessment of the measures set out in this Article.

CHAPTER VI: SHARING, TRANSFER, STORAGE AND RETENTION OF PERSONAL DATA

Article 48: Sharing and transfer of personal data outside Rwanda

The data controller or the data processor may

share or transfer personal data to a third party outside Rwanda if:

- 1° he or she has obtained authorisation from the supervisory authority after providing proof of appropriate safeguards with respect to the protection of personal data;
 - 2° the data subject has given his or her consent;
 - 3° the transfer is necessary:
 - a. for the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures taken in response to the data subject's request;
 - b. for the performance of a contract concluded in the interest of the data subject between the data controller and a third party;
 - c. for public interest grounds;
 - d. for the establishment, exercise or defence of a legal claim;
 - e. to protect the vital interests of the data subject or of another person where the data subject is physically or legally
-

incapable of giving his or her consent;

- f. for the purposes of compelling legitimate interests pursued by the data controller or by the data processor which are not overridden by the interests, rights and freedoms of the data subject, and when:
 - i. the transfer is not repetitive and concerns only a limited number of data subjects;
 - ii. the data controller or the data processor has assessed all the circumstances surrounding the data transfer and has, on the basis of that assessment, provided suitable safeguards with regard to the protection of personal data;
- g. for the performance of international instruments ratified by Rwanda.

The supervisory authority may put in place a regulation determining another reason of sharing or transferring personal data to a third party outside Rwanda.

Article 49: Contract for transfer of personal data

The data controller or the data processor who authorises a person to access personal data, share or transfer them to a third party outside Rwanda, enters into a written contract with such a person setting out the respective roles and responsibilities of each party to ensure compliance with this Law.

The supervisory authority may, by a regulation, determine the form of the contract to be used for transfers of personal data outside Rwanda.

Provisions of Items 1° and 3° a), b) and d) of Article 48 of this Law do not apply to activities carried out by a public body in the exercise of its functions.

The supervisory authority may require the data controller or the data processor to demonstrate their compliance with the provisions of this Article, and in particular, with personal data security safeguards and interests referred to in item 3° f) of Article 48 of this Law.

The supervisory authority, in order to protect the rights and freedoms of the data subject, may prohibit or suspend the transfer of personal data outside Rwanda.

Article 50: Storage of personal data

The data controller or the data processor stores personal data in Rwanda.

However, the storage of personal data outside Rwanda is only permitted if the data controller or the data processor holds a valid registration certificate authorising him or her to store personal data outside Rwanda, which is issued by the supervisory authority.

Article 51: Migration and management of personal data after change or closure of business

The supervisory authority puts in place a regulation determining modalities for migration and management of personal data in case of change or closure of business of the data controller or the data processor.

Article 52: Retention of personal data

The data controller or the data processor retains personal data until the purposes of the processing of personal data are fulfilled.

However, the data controller or the data processor may retain personal data for a longer period for the following grounds:

- 1° if retention is authorised by Law;
- 2° if retention is required by a contract concluded between the parties;
- 3° if the personal data is related to a function or activity for which the personal data are collected or processed;
- 4° preventing, detecting, investigating, prosecuting or punishing an offender;
- 5° protecting national security;
- 6° enforcing a court order;

- 7° enforcing legislation relating to collection of public revenues;
- 8° conducting proceedings before a court;
- 9° carrying out research authorised by a relevant authority;
- 10° if the data subject consents.

The supervisory authority may put in place a regulation determining any other ground for retention of personal data for a longer period.

At the end of the personal data retention period, the data controller or the data processor must destroy the personal data in a manner that prevents its reconstruction in an intelligible form.

**CHAPTER VIII: MISCONDUCTS,
OFFENCES AND SANCTIONS**

**Section One: Administrative misconducts
and sanctions**

Article 53: Administrative misconducts

The data controller, the data processor or a third party who commits one of the following misconducts:

- 1° failure to maintain records of processed personal data;
- 2° failure to carry out personal data logging;
- 3° operating without a registration certificate;
- 4° failure to report a change after receiving a registration certificate;
- 5° using a certificate whose term of validity has expired;
- 6° failure to designate a personal data protection officer;

- 7° failure to notify a personal data breach;
- 8° failure to make a report on personal data breach;
- 9° failure to communicate a personal data breach to the data subject;

commits a misconduct.

He or she is liable to an administrative fine of not less than two million Rwandan francs (RWF 2,000,000) but not more than five million Rwandan francs (RWF 5,000,000) or one percent (1%) of the global turnover of the preceding financial year.

In the event of a corporate body or a legal entity, he or she is liable to one percent (1%) of the global turnover of the preceding financial year.

The supervisory authority may put in place a regulation determining other administrative misconducts and sanctions that are not provided for in this Law.

Article 54: Filing an application to the court

The data controller, the data processor or a third party who is not satisfied with administrative sanction taken against him or her has the right to file an application to the competent court.

Article 55: Place where the administrative fine is deposited

The administrative fine imposed by the supervisory authority is deposited to the Public Treasury.

Section 2: Offences and penalties

Article 56: Accessing, collecting, using, offering, sharing, transfer or disclosing of personal data in a way that is contrary to this Law

A person who accesses, collects, uses, offers, shares, transfers or discloses personal data in a way that is contrary to this Law, commits an offence.

Upon conviction, he or she is liable to an imprisonment of not less than one (1) year but not more than three (3) years and a fine of not

less than seven million Rwandan francs (RWF 7,000,000) but not more than ten million Rwandan francs (RWF 10,000,000) or one of these penalties.

Article 57: Re-identification of de-identified personal data in a way that is contrary to this Law

Any person who knowingly, intentionally or recklessly:

- 1° re-identifies personal data which have been de-identified by a data controller or a data processor;
- 2° re-identifies and processes personal data, without consent of the data controller;

commits an offence.

Upon conviction, he or she is liable to an imprisonment of not less than one (1) year but not exceeding three (3) years and a fine of not less than seven million Rwandan francs (RWF 7,000,000) but not more than ten million Rwandan francs (RWF 10,000,000) or one of these penalties.

Article 58: Destruction, erasure, concealment or alteration of personal data in a way that is contrary to this Law

A person who destroys, erases, conceals or alters personal data in a way that is contrary to this Law, commits an offence.

Upon conviction, he or she is liable to an imprisonment of not less than three (3) years but not more than five (5) years and a fine of not less than seven million Rwandan francs (RWF 7,000,000) but not more than ten million Rwandan francs (RWF 10,000,000) or one of these penalties.

Article 59: Sale of personal data in a way that is contrary to this Law

A person who sells personal data in a way that is contrary to this Law, commits an offence.

Upon conviction, he or she is liable to an imprisonment of not less than five (5) years but not more than seven (7) years and a fine of not less than twelve million Rwandan francs (RWF 12,000,000) but not more than fifteen million Rwandan francs (RWF 15,000,000) or

one of these penalties.

Article 60: Collecting or processing of sensitive personal data in a way that is contrary to this Law

A person who collects or processes sensitive personal data in a way that is contrary to this Law, commits an offence.

Upon conviction, he or she is liable to an imprisonment of not less than seven (7) years but not more than ten (10) years and a fine of not less than twenty million Rwandan francs (RWF 20,000,000) but not more than twenty-five million Rwandan francs (RWF 25,000,000) or one of these penalties.

Article 61: Providing false information

A person who provides false information during and after registration, commits an offence.

Upon conviction, he or she is liable to an imprisonment of not less than one (1) year but not more than three (3) years and a fine of not less than three million Rwandan francs.

RWF 3,000,000) but not more than five million Rwandan francs (RWF 5,000,000) or one of these penalties.

Article 62: Punishment of a corporate body or a legal entity

A corporate body or a legal entity that commits one of the offences referred to in Articles 56, 57, 58, 59, 60 and 61 commits an offence.

Upon conviction, it is liable to a fine of Rwandan francs amounting to five percent (5%) of its annual turnover of the previous financial year.

Article 63: Additional penalties

In addition to penalties provided for in this Law, the court, in all cases, may order the seizure or confiscation of items used in the commission of any of the offences provided for in this Law and the proceeds gained.

The court may also order permanent or temporary closure of the legal entity or body, or the premises in which any of the offences provided for under this Law was committed.

**CHAPTER IX: MISCELLANEOUS
TRANSITIONAL AND FINAL
PROVISIONS**

**Article 64: Organ in charge of settlement of
conflicts**

The supervisory authority is the organ in charge of settlement of conflicts that may arise in relation to this Law.

However, a person who is not satisfied with the settlement of conflicts referred to in Paragraph one of this Article may file a case with the competent court.

Article 65: Right to claim for compensation

A person who suffers serious damage due to acts of a data controller or a data processor in violation of this Law has the right to claim for compensation with a competent court.

However, the data controller or the data processor is exempt from liability if he or she proves that he or she was not responsible for the damage.

Article 66: Power to put in place regulations

The competent authority may, in conjunction with the supervisory authority, put in place other sector-specific regulations governing the protection of personal data and privacy.

The regulations referred to in Paragraph One of this Article must comply with the provisions of this Law.

Article 67: Transitional period

The data controller or the data processor who is already in operation has a period not exceeding two (2) years from the date of publication of this Law in the Official Gazette of the Republic of Rwanda to conform his or her operations to the provisions of this Law.

Article 68: Drafting, consideration and adoption of this Law

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

Article 69: Repealing provision

All prior legal provisions contrary to this Law are repealed.

Article 70: Commencement

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

(sé)

KAGAME Paul

Perezida wa Repubulika
President of the Republic
Président de la République

(sé)

Dr NGIRENTE Edouard

Minisitiri w'Intebe
Prime Minister
Premier Ministre

kandi bishyizweho Ikirango cya Repubulika
and sealed with the Seal of the Republic:
u et scellé du Sceau de la République:

(sé)

Dr UGIRASHEBUJA Emmanuel

Minisitiri w'Ubutabera akaba n'Intumwa Nkuru ya Let
Minister of Justice and Attorney General
Ministre de la Justice et Garde des Sceaux
