RWANDA
UTILITIES
REGULATORY
AUTHORITY

Inspiring development

REGULATION N^{O} ...../…../ICT/RURA/019 OF ...../...../2019 GOVERNING THE USE OF PERSONAL DATA IN RWANDA

ADOPTED BY THE
REGULATORY BOARD
OF

RWANDA UTILITIES REGULATORY AUTHORITY (RURA)

CONTENTS

CHAPTER I . GENERAL PROVISIONS 5
Article 1: Purpose of this Regulation 5
Article 2:Scope of application 5
Article 3. Definition of terms 5
Article 4: Objective of this Regulation 8
CHAPTER II. PRINCIPLES OF DATA PROTECTION 8
Article 5: Grounds for lawful processing of personal data 8
Article 6: Purpose limitation 9
Article 7: Data minimisation 9
Article 8: Data Accuracy 9
Article 9: Data storage limitation 9
Article 10: Integrity and confidentiality 9
CHAPTER III. REQUIREMENTS TO COLLECT AND PROCESS PERSONNAL DATA 10
Section One: General Requirements 10
Article 11: Privacy of the data subject 10
Article 12: Consent to collect or process personal data 10
Article 13: Conditions for consent 10
Article 15: Right to withdraw 11
Article 16: Conditions applicable to child's consent in relation to information society services 11
Article 17:. Prohibition on Collecting and processing sensitive personal data 11
Article 18: Safeguards to process sensitive personal data 12
Article 19: Processing personal data relating to criminal convictions 12
Article 20 : Processing data without requiring an identification 12
Article 21: Collection of data from data subject 12
Article 22: Information to be given to data subject before collection of data 13
Section 2: Quality Information and Record of Personal Data 13
Article 23. Data quality 13
Article 24. Correction, deletion and destruction of personal data 13
Article 25 : Logging 14
Article 26: Retention of records of personal data 14
Article 27: Right to be forgotten 15
Article 28: Restriction of processing personal data 16
Article 29: Data processing records 16

CHAPTER IV. PROCEDURES FOR DATA SHARING 17
Article 30: Obtaining access to personal data 17
Article 31: Eligibility to access personal data 17
CHAPTER V: RESPONSIBILITIES OF THE REGULATORY AUTHORITY, THE DATA CONTROLLER AND DATA PROCESSOR 17
Article 32: Responsibilities of the Regulatory Authority 17
Article 33: Responsibilities of the data controller and data processor 18
CHAPTER VI. SECURITY OF PERSONAL DATA AND CROSSBORDER TRANSFER 18
Article 34: Security measures 18
Article 35: Personal Data Integrity 19
Article 36. Notification of data security breaches 19
Article 38 : Notification procedure on data subject 20
Article 39: Transfer of personal data outside Rwanda 21
Article 40: Authorization procedures 21
CHAPTER VII. RIGHTS OF THE DATA SUBJECT 21
Article 41: Right to access personal information 21
Article 42: Right to prevent processing of personal data 22
Article 43: Right to data portability 22
Article 44: Right to compensation 22
Article 45: Automated individual decision-making including profiling 22
CHAPTER VIII: ENFORCEMENT PROCEDURES AND ADMINISTRATIVE SANCTIONS 23
Section One: Enforcement and appeal procedures 23
Article 46: Enforcement Procedures 23
Article 47: Appeals to the Regulatory Authority 23
Section 2: Administrative sanctions 24
Article 48: Failure to comply with an enforcement notice 24
Article 49. Processing personal data without consent 24
Article 50: Collecting personal data from a third party 24
Article 51: Processing particular sensitive data 24
Article 52: Failure to notify a data breach 24
Article 53: Processing personal data abroad without authorization 24
CHAPTER IX. TRANSITIONAL AND FINAL PROVISIONS 25
Article 54: Repealing provision 25
Article 55: Commencement 25

PREAMBLE

Pursuant to the Constitution of the Republic of Rwanda of 2003 revised in 2015;

Considering deliberations from the consultative meeting held on ....., 2019 with stakeholders;

Pursuant to Law Nº09/2013 of 01/03/2013 establishing Rwanda Utilities Regulatory Authority (RURA) and determining its mission, powers, organisation and functioning especially in Article 2 (1°), 4 (1°), 6,; and 20 (1º);

Pursuant to Law n°24/2016 of 18/06/2016 governing information and communication technologies especially in Article 23, 124, 208, 209 and 213.

The Regulatory Board of the Rwanda Utilities Regulatory Authority in its meeting of……..;

HEREBY issues the following Regulation;

CHAPTER I . GENERAL PROVISIONS

Article 1: Purpose of this Regulation

The purpose of this Regulation is to enable every individual to exercise and have recourse to protection of their right to privacy and other related rights and freedoms in connection with personal data use in Rwanda and personal data of citizen of Rwanda being or to be processed abroad.

Article 2:Scope of application

This Regulation applies to all regulated sectors and their third parties that access, store, transfer, transmit and process data, whether done by electronic means or other means using personal data through an automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Article 3. Definition of terms

For the purpose of this regulation , the following terms must be defined as follows:

1. **Biometric data**: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
2. **Breach**: is a violation of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
3. **Consent of the data subject:** is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
4. **Data concerning health**: personal data related to the physical or mental health of an individual , including the provision of health care services, which reveal information about his or her health status;
5. **Data controller**: the natural or legal person, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

6. **Data processor:** is a natural or legal person or other body authorised by the data controller to process personal data;

7. **Data sharing**: refers to the use and/or disclosure of personal data to one or more organisation (s) and the latter's collection of that personal data;

8. **Data subject**: is an individual from whom or in respect of whom personal information has been requested, collected, collated, processed or stored;

9. **Electronic communications services:** a public service normally provided for remuneration which consists wholly or mainly in the transmission and routing of signals electronic communications networks;

10. **Genetic data**: personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

11. **Individual :** is any data subject identified or identifiable on the basis of his/her proper name, unique personal identification number, address code or any other distinguishing feature of his/her physical, psychological, spiritual, economic, cultural or social identity;

12. **Personal data:** is any information relating to an identified or identifiable individual;

13. **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;

14. **Pseudonymization** : refers to 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;

15. **Identifiable natural person**: is one 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, physiological, genetic, mental, economic, cultural or social identity of that individual ;

16. **Processing**: is 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, organisation, structuring, storage, adaptation or alteration retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

17. **Recipient**: is a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not;

18. **Regulatory Authority**: Rwanda Utilities Regulatory Authority (RURA);

19. **Sensitive personal data**: data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, traffic data, official identifier, transaction data, passwords, classified data, legal proceedings, penal or administrative sanctions;

20. **Subscriber:** a person who is a party to a contract with a provider for the supply of services;

21. **Subscriber's data:** any information that identifies or describes a particular Subscriber;

22. **Third party**: is any natural or legal person, public authority, agency or body other than the data subject, data controller, processor and persons who, under the direct authority of the data controller are authorised to process personal data;

23. **Use:** is the action of collecting, storing, sharing and processing personal data;

24. Vital interests: interest linked to life and/or death of data subject.

Article 4: Objective of this Regulation

The objective of this Regulation is to set out:

a) Conditions for collecting, storing, sharing and processing personal data ;
b) limitations of data controller and data processor on personal data;
c) enforcement mechanisms of this Regulation.

CHAPTER II. PRINCIPLES OF DATA PROTECTION

Article 5: Grounds for lawful processing of personal data

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
Processing shall be lawful only if :

a. the data subject gives consent to the processing of his or her personal data;

b. 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;

c. processing is necessary for compliance with a legal obligation to which the controller is subject;

d. processing is necessary to protect the vital interests of the data subject or of another individual;

e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;

f. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is considered to be compatible with the initial purposes.

Article 6: Purpose limitation

Data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Article 7: Data minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Article 8: Data Accuracy

Data must be accurate and where necessary, kept up to date.

Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Article 9: Data storage limitation

Personal data are required to 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.

Without prejudice to the preceding paragraph, personal data may be retained for a longer period of time if such retention is:

a) explicitly mandated, or necessary to comply with any obligation provided under a law or regulation into force;

b) for archiving purposes in the public interest;

c) for Scientific or historical research and statistical purposes;

The data controller or data processor shall undertake a periodic review to determine whether it is necessary or not to retain the personal data in its possession.

Article 10: Integrity and confidentiality

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The data controller shall ensure that data processor complies with the provision of the above paragraph.

CHAPTER III. REQUIREMENTS TO COLLECT AND PROCESS PERSONNAL DATA

Section One: General Requirements

Article 11: Privacy of the data subject

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

Article 12: Consent to collect or process personal data

Any data controller and/or processor shall require consent of the data subject prior to processing personal data.

Article 13: Conditions for consent

The data controller shall demonstrate that the data subject has consented to processing of his or her personal data.

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.
When assessing whether consent was freely given, the circumstances in which it was given must be taken into account.

Article 14: A written 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 form using a clear, plain and understandable official language to the data subject.

Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

Article 15: 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. It shall be as easy to withdraw as to give consent.

Article 16: Conditions applicable to child's consent in relation to information society services

The processing of the personal data of a child shall be lawful where the child, is at least 18 years old. Where the child is below that age, such processing shall be lawful only when it is given by the holder of parental responsibility over the child.

The data controller shall ensure that the consent is given by the holder of parental responsibility over the child

Article 17:. Prohibition on Collecting and processing sensitive personal data

It is prohibited to collect and process the data considered as sensitive personal data.

However, without prejudice to existing policies, laws and regulations, sensitive personal data may be collected and processed if:

a. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment and social aspect as it is authorized by the law into force in Rwanda;

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 18: 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 includes 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 personal data within the controller;
e. separate processing of such data;
f. the pseudonymization of personal data;
g. the encryption of personal data; or
h. Specific codes of conduct to ensure lawful processing in case of transfer or processing for other purposes.

Article 19: 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 National Public Prosecution Authority or when the processing is authorised by law into force, the processor must provide appropriate safeguards for the rights and freedoms of data subjects.

Any comprehensive register of criminal convictions shall be kept only under the control of National Public Prosecution Authority.

Article 20 : Processing data without requiring an identification

If the purposes for which a controller processes personal data do not or no longer require the identification of a data subject by the controller, 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 Regulation.

Article 21: Collection of data from data subject

A person shall collect personal data 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 necessary.

Article 22: Information to be given to data subject before collection of 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, 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 authorised requirement for the collection of the information or the requirement by law for its collection;
f. The recipients of the data;
g. The exercise of the right of access to and right to request rectification of the data collected before the collection;
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 23. Data quality

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

Article 24. 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 of the request and analysis of reasons for corrections, deletion or destruction of personal data, the data controller shall comply with the request or provide the data subject with a written reason for non-compliance with the request to the data subject.

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 correction made. The data controller shall notify the data subject of the action taken as a result of the request.

Article 25 : 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 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 data protection officer, the regulatory 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.

The data controller and the data processor shall make the logs available to the regulatory authority on request.

Article 26: Retention of records of personal data

Any person who collects or processes personal data shall retain them only for the length of period necessary to achieve the purposes for which they were collected and processed unless such retention is:

a. required or authorised by law;
b. required by a contract between the parties to the contract;
c. Agreed upon by the data subject.

Notwithstanding the provision of this article, personal data shall be 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 monetary penalty;
d. The enforcement of legislation relating to public revenue collection;
e. The conduct of proceedings before any court or tribunal;

Article 27: Right to be forgotten

A 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 public, he 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, the right to be forgotten 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.

<u>Article 28</u>: Restriction of processing personal data

A controller may, at the request of a data subject, restrict the processing of personal data 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 controller no longer needs the personal data for the purpose of the processing, but the data subject requires them for the establishment, exercise or defense of a legal claim;
c. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or
d. 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.

The controller shall implement mechanisms to ensure that the time limits established for erasure or restriction of processing of personal data, or for a periodic review of the need for the storage of the personal data, are observed.

<u>Article 29</u>: Data processing records

The data controller shall establish and maintain records containing the following basic information:

a. type of data and name of data file;
b. type of procesing activities;
c. business name, name, head office and address of the data processor;
d. date of commencement of data processing or date of data file creation;
e. the purpose of processing;
f. the legal grounds for data processing or creation of data file;
g. the category of data subjects;
h. the type and degree of data confidentiality;
i. the method of data collection and keeping;
j. the time limit for data keeping and use;
k. safeguards put in place to protect data;
l. requests concerning data processing.

The data controller shall update the records whenever a change occurs in relation to the basic data.

CHAPTER IV. PROCEDURES FOR DATA SHARING

Article 30: Obtaining access to personal data

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

If the data controller rejects the request, the rationale of this decision must specify the reasons for rejection, as well as the reasons why processing is not allowed.

Article 31: Eligibility to access personal data

A data processor is eligible to access personal data , only if :

a. It is an entity incorporated under the Law in Rwanda and has known address;
b. It has a valid company registration certificate;
c. It has a contract or a recommendation from the Government institution.
d. It holds a valid contract expressing the data subject's consent to process his personal data; and
e. Presents documents that clearly demonstrates how the requested data are going to be used and the outcome of that processing.

CHAPTER V: RESPONSIBILITIES OF THE REGULATORY AUTHORITY, THE DATA CONTROLLER AND DATA PROCESSOR

Article 32: Responsibilities of the Regulatory Authority

The regulatory authority must ensure that every data controller, data processor or any other person collecting or processing data within regulated sector complies with the principles of data protection.

The Regulatory Authority shall:

a. authorize the data processor to undertake the activity of data processing inside and outside Rwanda;
b. monitor and ensure compliance of this Regulation;
c. promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing personal data;
d. upon request, provide information to any data subject concerning their rights under this Regulation;

e. Facilitate and handle complaints lodged by a data subject, or by a body, organisation or association, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation.
f. monitor relevant developments related to protection of personal data and amend this regulation accordingly where necessary;
g. define minimum standard contractual clauses and ensure their compliance;
h. establish and maintain a list in relation to the requirement for data protection impact assessment;
i. Incite and enable development of codes of conduct for the data processing entities, and provide an opinion and approve such codes of conduct which provide sufficient safeguards;
j. keep internal records of infringements of this Regulation and of measures taken.

Article 33: Responsibilities of the data controller and data processor

Any data controller, data processor or any person who collects, processes, holds or uses personal data must :

a. be accountable to the subject for data collected, processed, held or used;
b. collect and process data fairly and lawfully;
c. retain personal data for the period authorised by this Regulation and relevant laws into force in Rwanda or for which the data is required;
d. ensure accuracy of information collected, processed, used or held;
e. ensure transparency and get consent prior to the collection, processing, use and holding of the personal data;
f. ensure privacy of collected, processed, used or held personal data
g. observe security safeguards in respect of the data;
h. comply with any other any directive set by the Regulatory authority.

CHAPTER VI. SECURITY OF PERSONAL DATA AND CROSSBORDER TRANSFER

Article 34: Security measures

Any data controller and data processor shall secure the integrity of personal data in possession or under his control by adopting appropriate, reasonable, technical and organisational measures to prevent loss, damage, or unauthorised processing of the personal data.

The data controller and data processor shall take measures to:

a. identify reasonable foreseeable internal and external risks to personal data his possession or under his control;
b. establish and maintain appropriate safeguards against the identified risks;
c. regularly verify that the safeguards are effectively implemented;
d. ensure that the safeguards are continually updated in response to new risks or deficiencies.

Article 35: Personal Data Integrity

A data controller shall not permit a data processor to process personal data, unless the data processor establishes and complies with the security measures specified under this Regulation. A contract between a data controller and a data processor relating to processing personal data, must require the data processor to establish and maintain the confidentiality and security measures necessary to ensure the integrity of the personal data.
Prior the signature, the regulatory authority must first approve such contract.

Article 36. Notification of data security breaches

Where the data controller or data processor or any other individual believes that the personal data of a data subject has been accessed or acquired by an unauthorised person and after verification, the data processor or data controller must immediately take remedial action, evaluate the nature and scope of the breach and whether the breach is likely to cause harm to data subjects.

The data controller or data processor shall notify the Regulatory Authority and other concerned authorities as soon as the data breach is noticed and report in prescribed manner, within twenty four (24) hours, remedial actions taken .

The Regulatory Authority must determine and notify the data controller or data processor, whether or not the data subject should be notified of the breach.

Article 37: Failure to notify the breach

Where the data controller or data processor fails to notify the Regulatory Authority of the data breach within the time limit specified under this Regulation, he/she shall provide the regulatory authority with the reasons for the delay.

The notification 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 data controller or data processor shall specify the facts relating to the personal data breach, its effects and the remedial action taken so as to enable the Regulatory Authority to verify compliance. The information provided to the Regulatory Authority must be true and accurate to the best knowledge of the data controller or data processor.

Article 38 : Notification procedure on data subject

Where the Regulatory Authority determines that the data controller or data processor should notify the data subject, such notification shall be made through:

a. registered mail to the data subject's last known residential or postal address;
b. telephone call, text message or electronic mail to the data subject's last known addresses;
c. placement in a prominent position on the website of the responsible party ; and
d. publication in the mass media.

Any notification must provide sufficient information to allow the data subject to take protective measures against the consequences of unauthorised access of acquisition of the data. Where the Regulatory Authority has grounds to believe that publicity would protect the data subject affected by the unauthorised access or acquisition of data, the Regulatory Authority ensure the responsible party publicises, in the specified manner, the fact of the compromise to the integrity or confidentiality of the personal data.

Article 39: Transfer of personal data outside Rwanda

Unless explicitly authorized by the Regulatory Authority, no personal data is allowed to be transferred, stored and processed outside the country.

Article 40: Authorization procedures

The data controller or data processor requesting for authorization to transfer, store or process the data outside Rwanda shall write to the Regulatory Authority requesting an authorization to do so.

The data controller shall justify the reason why the operations to be performed on that data, cannot be performed inside the country.
Upon the result of its assessment, the Regulatory Authority may grant or not the authorization requested.

the Regulatory Authority does not grant such authorisation, it responds in writing the reasons for the refusal.

CHAPTER VII. RIGHTS OF THE DATA SUBJECT

Article 41: Right to access personal information

A data subject who provides proof of identity may request a data controller or data processor to:

a. provide the purposes of the processing;
b. provide them with a copy of the data about the data subject;
c. confirm whether or not the data controller holds personal data about that data subject;
d. 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;
e. 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;
f. be informed of the source of data where the personal data were not collected from the data subject;
g. Inform the data subject in case personal data are transferred to a third country or to an international organisation;

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

Article 42: Right to prevent processing of personal data

The data subject shall 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 distess to the data subject;

The data controller shall within a period of fifteen days (15) after receipt of the notice inform the concerned data subject in writting that the data controller has complied or intends 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 Regulatory Authority.

Article 43: Right to data portability

The data subject shall have the right to have the personal data transmitted directly from one data controller to another, where technically feasible.

This right shall not adversely affect the rights and freedoms of others.

Article 44: Right to compensation

The data subject shall have right to seek compensation in case the controller or processor has caused a data subject to suffer damage by processing personal data in violation of this regulation or other law applicable to this processing. This right to seek compensation shall not apply if, in the case of non-automated processing, the damage was not the result of fault by the controller.

The data subject may request appropriate financial compensation for non-material damage. The Regulatory authority shall determine the appropriate financial compensation upon receipt and assessment of the complaint from the data subject.

Article 45: Automated individual decision-making including profiling

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 or significantly affects him.
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.

CHAPTER VIII: ENFORCEMENT PROCEDURES AND ADMINISTRATIVE SANCTIONS

Section One: Enforcement and appeal procedures

Article 46: Enforcement Procedures

Where the Regulatory Authority establishes that a data controller or data processor has contravened this regulation, the Regulatory Authority shall undertake enforcement proceedings against the controller or data processor;

The data controller and/or the data processor must comply with investigation procedures and requirements as well as any information requests instituted by the Regulatory Authority.

Article 47: Appeals to the Regulatory Authority

Any data controller or data processor on whom an enforcement notice is served may appeal to the Regulatory Authority against such enforcement notice or any part thereof.

Any data controller or data processor who wishes to appeal under this regulation must lodge a notice of appeal with the Regulatory Authority not later than seven working days (7) after the enforcement notice is served.

Such action of appeal shall not have the effect of suspending the operation of the enforcement notice or any part of the enforcement notice under appeal.

Any data controller or data processor not satisfied by the decision made by the Regulatory Authority may seek redress from competent courts of law in Rwanda.

Section 2: Administrative sanctions

Article 48: Failure to comply with an enforcement notice

Any data controller or data processor that contravenes an enforcement notice of the Regulatory Authority issued under provisions of this Regulation is liable to an administrative fine of between five hundred thousand (5,000,000) and fifteen million (15,000,000) Rwanda francs for each day of its non-compliance to the requirements, as of the day of confirmed notification;

Article 49. Processing personal data without consent

Any data controller or data processor that processes data without consent, is liable of a fine between five million (5,000,000) and ten million (10,000,000) Rwandan Francs.

Article 50: Collecting personal data from a third party

Any data controller or data processor that collects data from a third party, is liable of a fine between five million (5,000,000) and ten million (10,000,000) Rwandan Francs.

Article 51: Processing particular sensitive data

Any data controller or data processor that processes particularly sensitive data contrary to the provisions of this Regulation is liable of a fine between ten million (10,000,000) and fifteen million (15,000,000) Rwandan Francs.

Article 52: Failure to notify a data breach

Any data controller or data processor who intentionally fails to notify the regulatory authority of the data breach, is liable of a daily fine of between one million (1,000,000) and five million (5,000,000) Rwandan Francs, for each day calculated from the day the breach occurred.

Article 53: Processing personal data abroad without authorization

Any data controller or data processor who processes or stores personal data outside Rwanda without authorization, is liable of a daily fine of between ten million (10,000,000) and twenty million (20,000,000) Rwandan Francs, for each day calculated from the day the processing or storage of data started.

CHAPTER IX. TRANSITIONAL AND FINAL PROVISIONS

Article 54: Repealing provision

All prior provisions contrary to this regulation are hereby repealed.

Article 55: Commencement

This regulation shall come into force on the date of their signature by the Chairperson of the Regulatory Board. It must be publish in N.O.G

Done at Kigali on ...../...../ 2019

Dr. Ignace Gatare,
Chairperson of the Regulatory Board