DPO

Rwanda's
Data Protection Office

Frequently asked questions by Data Controllers and Data Processors

January 2023

www.dpo.gov.rw

9080

TABLE OF CONTENTS

AIM OF THE PERSONAL DATA PROTECTION & PRIVACY LAW

To strengthen the control and personal autonomy of data subjects over their personal data, thereby contributing to respect for their human rights and fundamental freedoms. This particularly relates to their right to privacy, which goes in line with international data protection standards, and is vital for modern digital economy facilitating services such as e-commerce, international financial transactions, and various online services.

The primary goals of this law are to:

- Empower citizens with agency over their personal data
- Enable trusted and secure data flows, domestically and internationally
- Provide regulatory certainty for existing businesses and prospective investors, and an enabling environment for SME growth
- Accelerate Rwanda's ambitions towards a technology- enabled and data-driven economy

WHO DOES THIS LAW APPLY TO?

- Individuals and institutions established or residing in Rwanda, that process the personal data of individuals in Rwanda (not just citizens).

- Individuals and institutions established or residing outside of Rwanda, that process the personal data of individuals in Rwanda

WHO IS A DATA SUBJECT?

A data subject means is an identified or identifiable individual, 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.

WHAT DOES PERSONAL DATA MEAN?

Personal data means 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.

WHAT DOES PRIVACY MEAN?

Privacy is a fundamental right of a person to decide who can access his or her personal data, and when, where, why and how his or her personal data can be accessed.

WHAT DOES SENSITIVE PERSONAL DATA MEAN?

Sensitive personal data means any 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.

WHAT IS GENETIC INFORMATION?

Genetic data means personal data relating to the general characteristics of an individual which are inherited or acquired and which provide unique information about the physiology or health of the individual and which result, in particular, from an analysis of a biological sample from the individual in question.

WHAT IS BIOMETRIC INFORMATION?

Biometric data means any personal data relating to the physical, physiological or behavioral characteristics of an individual which allow his unique identification, including fingerprint mapping, facial recognition, and retina.

WHAT ARE SPECIAL CATEGORIES OF PERSONAL DATA?

Special categories of personal data mean personal data pertaining to — (a) Person's race; (b) his Religious or philosophical beliefs; (d) his Social origin; (e) Health status; (f) Sexual life or family details; (g) Genetic or biometric information; (h) Criminal records; (i) Medical records.

WHAT DOES PROCESSING MEAN?

It is 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.

WHO IS A CONTROLLER?

The person who or the public or private body or legal entity which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing.

WHO IS A PROCESSOR?

It is a person, public or private corporate body or legal entity, which is authorized to process personal data on behalf of the data controller.

HOW DO YOU DETERMINE WHETHER YOU ARE A CONTROLLER OR PROCESSOR?

It is important to remember that an organization is not by its nature either a controller or a processor. Instead you need to consider the personal data and the processing activity that is taking place, and consider who is determining the purposes and the manner of that specific processing.

You need to ask yourself do I decide:

- to collect personal data in the first place;
- the lawful basis for doing so;
- what types of personal data to collect;
- the purpose or purposes the data are to be used for;
- which individuals to collect data about;
- whether to disclose the data, and if so, to whom;
- what to tell individuals about the processing;
- how to respond to requests made in line with individuals' rights; and
- how long to retain the data or whether to make non-routine amendments to the data.

These are all decisions that can only be taken by the controller as part of its overall control of the data processing operation. If you make any of these decisions determining the purposes and means of the processing, **you are a controller**.

If you find yourself; following instructions from someone else regarding the processing of personal data, given the personal data by a customer or similar third party or told what data to collect, not deciding to collect personal data from individuals or what personal data should be collected from individuals **you are a processor**.

IS IT POSSIBLE TO BE BOTH A CONTROLLER AND PROCESSOR?

Yes. In contexts where the data processor has the authority to process personal data for a separate purpose from that originally given by the data controller, the data processor becomes a controller in his or her own right for that element of data processing.

Additionally, in situations where an institution both determines the means of processing and processes the data itself, this entity becomes both a data controller and data processor.

Any natural person, public or private corporate body or legal entity, can be both a controller and processor of personal data when they are carrying out the activities of both roles.

WHAT IS THE SUPERVISORY AUTHORITY?

The supervisory authority is a public authority that is charged with enforcement of this law relating to the protection of personal data and privacy. This law designates the National Cyber Security Authority (NCSA) as the supervisory authority.

WHAT ARE THE POWERS OF SUPERVISORY AUTHORITY?

Article 28 of the law relating to the protection of personal data and privacy deals with the powers of the supervisory authority to carry out her functions under this law. These powers include issuing registration certificates and imposing administrative sanctions are among others.

SHOULD DATA CONTROLLERS AND DATA PROCESSORS REGISTER WITH SUPERVISORY AUTHORITY?

Yes. Article 29 of the law relating to the protection of personal data and privacy deals with the registration of data controllers and data processors. Anyone who intends to be a data controller or a data processor must register with the supervisory authority.

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 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.

WHAT IS CONSENT?

Consent of the data subject is 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.

HOW TO ENSURE THAT THE CONSENT MEET THE LEGAL REQUIREMENTS?

- Consent should be specific, informed and unambiguous, by setting out the purpose of the various phases of the processing.
- Consent should be easy to withdraw without affecting the lawfulness of processing.
- Consent should be made in oral, written or electronic form.
- Consent should be in one of the official languages that is understandable to data subject.
- At the time of collection, data subjects should be informed about the right to withdraw consent at any time.

DOES THIS LAW FEATURE ANY SPECIAL PROVISIONS FOR CHILDREN?

Yes, it does, the law states, in its Article 9, that 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.

WHY YOUR INSTITUTION NEEDS A DATA PROTECTION OFFICER

One of the provisions of the law on personal data protection and privacy indicates the need to designate a data protection officer (DPO) for any processing of personal data (Article 40).

Whether your institution acts as a data controller, data processor, or both of these roles, this law makes it mandatory to designate the DPO. Failure to designate a personal data protection officer is an administrative misconduct (Article 53).

WHAT ARE THE DUTIES OF DATA PROTECTION OFFICER?

The principal duties a data protection officer holds according to article 40 are:

- 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.
- 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.
- To provide advice were requested as regards the data protection impact assessment and monitor its performance.
- 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.

HOW THIS LAW CATERS FOR THE RIGHTS OF DATA SUBJECTS?

Chapter II of the law relating to the protection of personal data and privacy stipulates the rights of data subjects. The Act has enhanced the rights of data subjects by giving substantial rights including:

1. Right of the data subject to withdraw the consent (Article 8)
2. Right to personal data (Article 18)
3. Right to object (Article 19)
4. Right to data portability (Article 20)
5. Right to not be subject to a decision based on automated data processing (Article 21)
6. Right to restriction of processing of personal data (Article 22)
7. Right to erasure of personal data (Article 23)
8. Right to rectification (Article 24)
9. Right to designate an heir to personal data (Article 25)
10. Right to representation (Article 26)

Where the data controllers, the data processors know that personal data belong to a child under the age of sixteen (16) years they must obtain the consent of a holder of parental responsibility over the child in accordance with relevant Laws. Other exceptions are highlighted in the article 9.

WHAT ARE THE OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS?

Chapter VI of the law relating to the protection of personal data and privacy relates to a number of obligations which have been imposed on data controllers and data processors to ensure that processing of personal data is done in a fair and lawful manner such as:

Principles relating to processing of personal data	Data controllers and data processors need to ensure that processing of personal data is lawful, fair, transparent, adequate, relevant, accurate, kept for as long as required and proportionate to the purposes for which it is being processed, and are processed in compliance with the rights of data subjects.
Duties of the data controller and the data processor	The data controller and data processor must ensure all personal data is processed in compliance with the law, and be able to demonstrate compliance through a series of measures including implementing appropriate technical and organizational measures, keeping a record of personal data processing operations, and designating a data protection officer amongst others.
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 information to be shared with the data subject during data collection are provided in the article 42.
Notification of personal data breach	As soon as the data controller becomes aware that a breach has occurred, the controller must notify the breach to the supervisory authority within **forty-eight (48) hours** after having become aware of it. Where the data processor becomes aware of a personal data breach, he or she notifies the data controller **within forty-eight (48) hours** after being aware of the incident.

Report on personal data breach	The data controller draws up a report on personal data breach and submits it to the supervisory authority not later than **seventy-two (72) hours** with all facts available. The report content format is described in article 44.
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, there are some exceptions highlighted in ~~the~~ article 45.
Lawful processing of personal data	The law lays down the conditions for legal basis required for processing in the article 46.
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. The measures to ensure security of personal data are described in article 47.

WHAT DOES THE LAW SAY ABOUT STORAGE, TRANSFER, AND RETENTION OF PERSONAL DATA?

Chapter VII of the law relating to the protection of personal data and privacy deals with storage, transfer and retention of personal data.

Storage of personal data	The data controller or 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 authorization which is issued by the supervisory authority.
Sharing and transfer of personal data outside Rwanda	The data controller or data processor may share or transfer personal data to a third party outside Rwanda if an authorization has been obtained from the supervisory authority. Other conditions are described in article 48 and 49.
Migration and management of personal data after change or closure of business	In case of change or closure of business of the data controller or data processor, the supervisory authority puts in place a regulation determining modalities for migration and management of personal data.
Retention of personal data	The data controller or data processor retains personal data until the purposes of the processing of personal data are fulfilled. However, there are some exceptions highlighted in article 52.

IS IT AN OFFENCE NOT TO COMPLY WITH THE DATA PROTECTION ACT?

Yes. Offences, administrative misconducts and their respect penalties and sanctions are shown below:

Offences:					
Accessing, collecting, using, offering, sharing, transfer or disclosing of personal data in a way that is contrary to this Law	Re-identification of de-identified personal data in a way that is contrary to this Law	Destruction, erasure, concealment or alteration of personal data in a way that is contrary to this Law	Sale of personal data in a way that is contrary to this Law	Collecting or processing of sensitive personal data in a way that is contrary to this Law	Providing false information
Article. 56	Article. 57	Article. 58	Article. 59	Article. 60	Article. 61

Penalties:

- A controller or processor that commits one of the offences referred to in above 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.
- 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.

Administrative misconducts:
failure to maintain records of processed personal data
failure to carry out personal data logging
operating without a registration certificate
failure to report a change after receiving a registration certificate
using a certificate whose term of validity has expired
failure to designate a personal data protection officer
failure to notify a personal data breach
failure to make a report on personal data breach
failure to communicate a personal data breach to the data subject

Sanctions:

- A Data controller or data processor 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.

WHAT ARE IMPORTANT DOCUMENTS TO HAVE IN PLACE?

Documents	Relevant Article in the Law
Data Subject Consent Form	Articles 6 and 7
Data Subject Consent Withdrawal Form	Article 8
Parental Consent Form & Parental Consent Withdrawal Form	Articles 9 and 8
Inventory of Processing Activities	Article 17
Privacy Notice	Article 42
Website Privacy Policy	Article 42
Cookie Policy	Article 42
Personal Data Protection Policy	Articles 42, 46 and 47
Data Protection Impact Assessment Register	Article 38
Data Retention Policy & Schedule	Article 52
Supplier/Third Party Data Processing Agreement	Articles 4, 5, 48 and 49
Data Breach Response and Notification Procedure	Articles 43, 44 and 45
Data Breach Register	Article 44
Data Breach Notification Form to the Data Subjects	Article 45
Data Breach Notification Form to the Supervisory Authority	Articles 43 and 44

WHAT ARE THE IMPLICATIONS OF THE LAW FOR DIFFERENT SECTORS?

- **On Already Acquired Data**

The data controller and data processor have a transitional period of up to **October 15, 2023**, to comply with provisions of the law on the processing of personal data (Article 67)

- **On New Collected Data**

The data controller is required to first register with the supervisory authority. Where the data processor is required to get authorization from the data controller and register with the supervisory authority. (Articles 4, 29 and 30)

- **Storage of personal data**

The data controller and data processor stores personal data in Rwanda.
A valid registration certificate is required to authorize the storage of personal data outside Rwanda. (Article 50)

- **Share/Transfer of personal data**

A valid registration certificate is required to authorize the sharing and transfer of personal data outside Rwanda. (Articles 48)

- **Internal Processes of an Institution**

Designation of a data protection officer and adopting appropriate, reasonable technical measures to prevent loss, damage or destruction of personal data. (Articles 40 and 47)

IS THE PROCESS TO REQUEST AUTHORIZATION (AS OUTLINED IN ARTICLES 48 AND 50 OF THE DPP LAW) INCLUDED IN THE REGISTRATION PROCESS AS A DATA CONTROLLER, OR IS THERE A SEPARATE PROCESS TO BE FOLLOWED?

There are two possible ways particularly on data processing and registration requirement for data transfer outside Rwanda:

1. Authorization provided for under Art.48 (1) of DPP law to transfer personal data outside Rwanda is done during registration to operate as a data controller or data processor;

This complements Art. 30 (7) DPP law requiring the applicant to indicate the country to which he/she intends to directly or indirectly transfer the personal data;

2. A request to transfer personal data outside Rwanda may also be submitted after registration for specific processing reasons of personal data outside Rwanda as the need may arise depending on the changing nature of the business/operations and other reasons described in Art. 48 (2-3) and also in consideration of the required appropriate safeguards as provided for by the Law.

Note: If the second scenario (2) comes in after registration, he/she will then be required to request for a change on the registration certificate.

WHO IS SUPPOSED TO REGISTER? DOES THE SIZE OF THE ORGANIZATION MATTER?

Anyone who is processing or who is willing to process personal data/whoever is already in personal data processing or wants to operate as a data controller or data processor.

WHAT IS DE-IDENTIFIED DATA?

It is the removal of personal identifiable information for the purpose of safeguarding personal data.

IS DE-IDENTIFIED DATA NO LONGER CONSIDERED PERSONAL?

It remains personal between data subject and the data controllers or processors. **i.e., De-identification** should be understood as a technique used to protect individual's privacy.

WHAT IS THE PROCEDURE IF PERSONAL DATA IS NOT FROM A NATURAL PERSON (WHAT IS A NATURAL PERSON)?

The Law applies to whoever processes personal data whether natural or moral person, whether directly received from the data subject by the data controller or indirectly received from the data controller by whoever processes data on his/her behalf.

A natural person is a physical person as opposed to moral person.

If you are a person, public or private corporate body or legal processing personal data for the following purposes you need to register as a data controller or a data processor with the National Cyber Security Authority (NCSA).

1. Charities and Religious entities.
2. Security companies (including operating security CCTV systems).
3. Gambling.
4. Operating an educational institution.
5. Health administration and provision of patient care.
6. Hospitality industry firms but excludes tour guides.
7. Property management including the selling of land.
8. Provision of financial services.
9. Telecommunications network or service providers.
10. Businesses that are wholly or mainly in direct marketing.
11. Transport services firms (including online passenger hailing applications)
12. Businesses that process genetic or/and biometric data.
13. Any businesses that deals with personal data.

Contact Details:

DATA PROTECTION OFFICE

18KG Ave, A&P Building, Ground Floor, Kacyiru, Kigali-Rwanda
Toll Free: 9080
Email: dpp@ncsa.gov.rw
Website: www.dpo.gov.rw