DPO

Rwanda's
Data Protection Office

Guidance on Personal Data Inventory and Readiness Checklist Tools

May 2023

www.dpo.gov.rw

9080

CONTENTS

1. INTRODUCTION

The law Nº 058/2021 of 13/10/2021 relating to the protection of personal data and privacy (DPP Law) was officially published in the Official Gazette of the Republic of Rwanda on 15th October 2021.

This law now brings Rwanda in line with international data protection standards, vital for the modern digital economy facilitating various online services.

The primary goals of DPP Law are to:

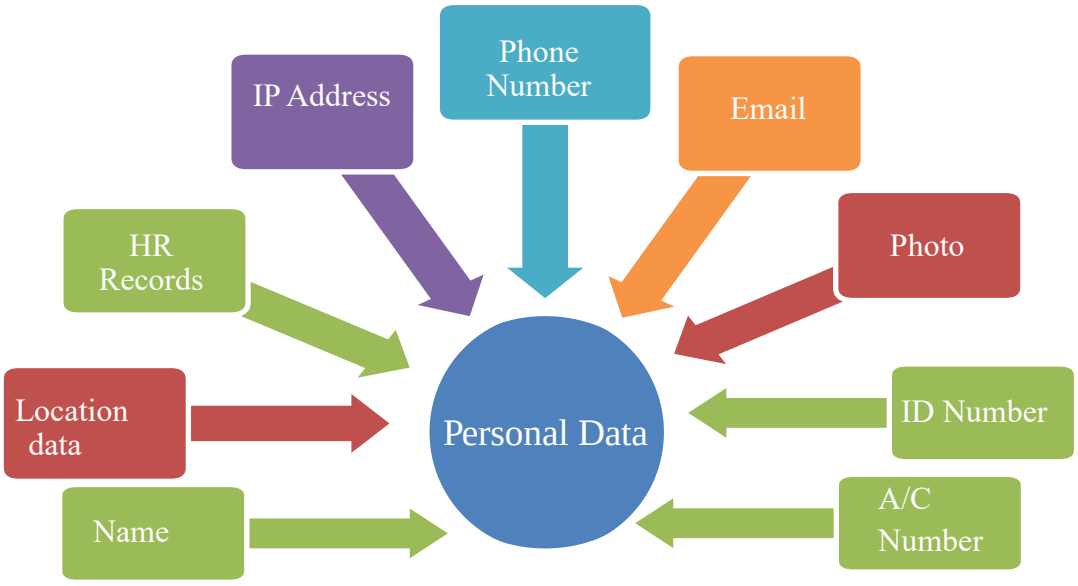
- Empower citizens with agency over their personal data
- Enable trusted and secure data flows, domestically and internationally
- Accelerate Rwanda's ambitions towards a technology enabled and data-driven economy

The DPP Law emphasizes transparency, security and accountability by organizations, while at the same time standardizing and strengthening the privacy rights of individuals in Rwanda.

This document has been designed along with other published guides to assist organizations to implement data protection and privacy compliant arrangements.

2. WHO DOES DPP LAW APPLY TO?

DPP Law is designed to help safeguarding rights for individuals in Rwanda, and introduces a single set of rules across Rwanda when it comes to how organizations handle data relating to identifiable individuals. If you are either established in Rwanda or outside Rwanda and process any of the following personal information, you would be subject to the requirements of the DPP Law.



All organizations, regardless of their size, are urged to get on the front foot when it comes to personal data protection and privacy standards. The standards that organizations implement should be proportionate to their data processing. This means that the Data Protection and Privacy Office will expect more robust arrangements from organizations that process large volumes of personal data, and/or personal data of a sensitive nature, than from organizations with largely inconsequential data processing activities.

The following are key steps that will help towards ensuring compliance with the DPP Law

1. **Designation of Data Protection Officer**
   The Data Protection Officer will help your organization to handle all matters related to processing of personal data including compliance monitoring with DPP Law. (Articles 40 & 41 of DPP law)

2. **Identify the personal data that you hold**
   All organizations must identify what personal data they hold. This can be achieved by setting out the information listed in Article 17 of the DPP Law.

3. **Registration with Data Protection and Privacy Office**
   All organizations intend to be a data controller or a data processor must register with the supervisory authority through Data Protection & Privacy Office (Article 29 of DPP Law)

4. **Conduct a risk assessment**
   This should include a risk assessment of the personal data you hold and your data processing activities.

5. **Implement appropriate technical & organizational measures**
   This must be done to ensure personal data (found on digital and paper files) is stored securely. The security measures your organization should put in place will depend on the type of personal data you hold and the risk associated to them (Article 11 of the DPP law).

6. **Lawful basis**
   Know the legal basis you rely on: is it consent? Is it a contractual obligation or legitimate interest? Your legal basis must justify your processing of personal data (Article 46 of the DPP Law)

7	**Data minimization, storage limitation and accuracy** Ensure that – • you are only collecting the minimum amount of personal data necessary for your organization; • you only keep it for as long as necessary; and • you use reasonable measures to keep data accurate.
8	**Purpose specification, retention and transparency** Be transparent about the reasons for collecting their personal data. Inform about the specific uses it will be put to and how long you need to keep their personal data on file. This notice may be portrayed on your website, on forms used to collect data.
9	**Special categories of personal data** Do you process sensitive personal data? If so, you should take extra precautions and identify appropriate grounds for processing sensitive personal data and Safeguards to process sensitive personal data (Articles 10 and 11).
10	**Rights of the data subject** All organizations must be able to facilitate requests from service-users wishing to exercise their rights under the DPP law, including rights of access, rectification, erasure, withdrawal of consent, data portability and the right to object to automated processing.
11	**Request and obtain approvals to store and transfer personal data abroad** All organizations must have additional authorizations to store and transfer/share personal data outside Rwanda. (Articles 48 - 50 of DPP Law)
12	**Updated policies** Where appropriate, organizations should ensure that they regularly update any policy/procedure documents that detail how the organization is meeting its personal data protection obligations. This will prove useful to demonstrate compliance and meet the requirements under the DPP law.

3. GLOSSARY

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;

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;

Data Processor

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

Data Protection Impact Assessment (DPIA)

Describes a process designed to identify risks arising out of the processing of personal data and minimization of these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance, including ongoing compliance, with the DPP law.

Data Subject

A natural person from whom or in respect of whom, personal data has been requested and processed.

Lawful Basis

In order to process personal data, you must have a lawful basis to do so. The lawful grounds for processing personal data are set in the DPP law.

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.

Processing of personal Data

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 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.

Retention Policy

How long will your organization hold an individual's personal data? Your retention period will be influenced by several factors. There may be legal or other requirements on your organization, which may vary depending on your organization type, but data should not be retained *longer than necessary*, in relation to the purpose for which such data is processed. Further, data must be stored securely while it is in your possession and you must ensure it is deleted fully and safely at the appointed time.

Sensitive Personal Data

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.

4. INVENTORY AND READINESS TOOLS

The DPP Law might seem like looming giants to organization, it doesn't have to be daunting. Ignoring personal data protection and privacy law will not make it go away, so it is important to make sure organization understands what the DPP Law means to your organization specifically, and seek out the right resources to help you prepare and comply.

To assist, your organization, The Data Protection & Privacy Office prepared the Guidance Note includes the following:

Personal Data Inventory Tool

This tool will allow organizations to map out the personal data they hold and process. It will serve as a starting point to create an inventory in relation to the categories of the personal data processed, the lawful basis for each processing purpose(s), the retention period(s) and what, if any, remedial action is required to ensure compliance with personal data protection and privacy law **(Annex A).**

Readiness Assessment Checklist

After completing using the Personal Data Inventory Tool, this checklist provides a general means for organizations to ensure that the right measures (both organizational and technical) are taken, and at the same time, get an idea about their effectiveness. Aside from being a thought-provoking exercise, this assessment will allow organizations to further analyze their data protection capabilities, establish what measures they have in place and what else they must do to ensure compliance with personal data protection and privacy law **(Annex B).**

ANNEX A –PERSONAL DATA INVENTORY TOOL

Categories of personal data and data subjects	Elements of personal data included with each data category	Source of the personal data	Purposes for which personal data is processed	Lawful basis for each processing purpose	Special categories of personal data/data relating to criminal convictions	Lawful basis for processing sensitive personal data	Retention period	Accuracy	Remedial action required to ensure compliance with data protection law
List categories of personal data collected & retained. *For example:* *Current employee data* *Retired employee data* *Customer data* *Marketing database to include data about other businesses* *CCTV footage.*	**List each type of personal data included within each category of personal data** *For example:* *Name* *Address(es)* *Banking details* *Business purchases/trans actions* *Medical details* *Stored video and images of events*	**List the source(s) of the personal data.** *For example:* *Whether the data was collected directly from individuals.* *Whether the data was collected indirectly, from third parties*	**Within each category of personal data, list the purposes for the data is collected & retained** *For example:* *Did you collect the data for marketing purposes?* *Was the data collected and stored as part of a service enhancement or research project?* *Did you collect the data for a volunteer's program or event?*	**For each purpose that personal data (nonspecial categories) is processed, list the legal basis on which it is based** *Establish whether you are processing the data under consent for example, or whether you intend to satisfy a contractual or legal obligation.*	**If special categories of personal data are collected & retained; it is important to set out details of the nature of the data** *For example:* *Person's race* *,* *Health status/medical records* *Social origin* *Religious/ philosophical beliefs,* *Political opinion,* *Genetic or biometric information* *Sexual life/ family details*	**List the lawful basis on which special categories of personal data are collected and retained** *Establish whether you are processing the data with explicit consent from the data subject.*	**For each category of personal data, list the period for which the data will be retained** *For example:* *Do you retain/store the data for a month?* *Are you required to retain the data for a year?* *As a general rule data must be retained for no longer than is necessary for the purpose for which it was collected in the first place.*	**How important is data accuracy? Where applicable, when will updates occur?**	**Identify actions that are required to ensure all personal data processing operations are DPP law compliant** *For example,* *this may include deleting data where there is no further purpose for retention*

ANNEX B – READINESS ASSESSMENT CHECKLIST

PERSONAL DATA

	Question	Yes	No	Comments/Remedial Action
Consent-based data processing	Have you reviewed your organization's mechanisms for collecting consent to ensure that it is freely given, specific and informed?			
	When seeking consent, has the individual chosen to agree to the processing of their data by way of statement or a clear affirmative action?			
	If personal data that you currently hold on the basis of consent does not meet the required standard under the DPP Law, have you re-sought the individual's consent to ensure compliance under the DPP Law?			
	Are procedures in place to demonstrate that an individual has consented to their data being processed?			
	Are procedures in place to allow an individual to withdraw their consent to the processing of their data at any given time?			
Children's Personal Data	Where online services are provided to a child, are procedures in place to verify the age of that child?			
	Are measures in place to get consent of a parent or legal guardian where required?			
Processing of data based on legitimate interest	If legitimate interest is a legal basis on which personal data is on legitimate interest processed, has your organization carried out a suitable analysis to ensure that the use of this legal basis is appropriate? *Your analysis must demonstrate that* ***(i)*** *there is a valid legitimate interest;* ***(ii)*** *the data processing is strictly necessary in pursuit of the legitimate interest; and* ***(iii)*** *the processing is not prejudicial to or overridden by the rights of the individual.*			

DATA SUBJECT RIGHTS

	Question	Yes	No	Comments/Remedial Action
Access to personal data	Is there a documented policy/procedure in place for handling Subject Access Requests (SARs)?			
	Is your organization able to respond to SARs within the one month deadline set by the DPP law?			
	Are you aware of what information can be provided via a SAR, the set response times or way of providing the requested information to the data subject?			
Data Portability	Are procedures in place to provide individuals with their personal data in a structured, commonly used and machine readable format?			
Deletion & Rectification	Are there controls/procedures in place to allow personal data to be deleted or rectified (if applicable)?			
Right to Restriction of Processing	Do you have controls/procedures in place to halt the processing of personal data where an individual has, on valid grounds sought the restriction of processing?			
Right to Object to Processing	Are individuals informed about their right to object to certain types of processing (i.e. direct marketing)?			
Profiling & Automated Processing	Where an automated decision is made which is necessary Processing for entering into, or performance of a contract, or based on explicit consent, are procedures in place to facilitate an individual's right to obtain human intervention and to content this decision?			

ACCURACY & RETENTION

	Question	Yes	No	Comments/Remedial Action
Purpose Limitation	Is personal data only used for the purpose(s) for which it was originally collected?			
Data Minimization	Do you agree that the data collected is limited to what is necessary for the purpose(s) for which it is processed and nothing further?			

Accuracy	Are procedures in place to ensure personal data is kept up-to-date and accurate?			
Retention	Are retention policies/procedures in place to ensure data is held for longer than is necessary?			
Other legal obligations governing retention	Is your organization subject to other rules that require a minimum retention period (e.g. medical records, tax)?			
	Do you have procedures in place to ensure data is destroyed securely, in accordance with your retention policies?			
Duplication of Records	Are there procedures to ensure that there is no unnecessary or unregulated Records duplication of records?			

TRANSPARENCY

	Question	Yes	No	Comments/Remedial Action
Being transparent with customers & employees	Are your service users fully informed of how you use their data?			
	Are your employees fully informed of how you use their data?			
	Are you able to advise your customers and/or employees about how their data is processed in a concise, transparent, intelligible and easily accessible form, using clear and plain language?			
	Where personal data is collected directly from the individuals, are procedures In place to provide them with the information listed in Article 42 of the DPP law?			
	If personal data is collected from third parties (that is, not directly obtained from the individuals), do you have procedures in place to provide the information?			
	When engaging with individuals, such as when providing a service for example, do you proactively inform the individuals of their privacy rights?			
	Is information about how transparent your organization is with regards privacy rights and compliance with DPP law principles published in an easy, accessible and readable format?			

OTHER OBLIGATIONS

	Question	Yes	No	Comments/Remedial Action
Supplier Agreements	Do you have agreements in place with suppliers and other third parties processing personal data on your behalf?			
	Are the above agreements reviewed to ensure all appropriate data protection requirements are included?			
Data Protection Officers (DPOs)	Did your organization appoint a DPO?			
	If your organization has decided that a DPO is not required, have you of the documented the reasons why?			
	Where a DPO is appointed, are escalation and reporting lines in place and have these procedures been documented?			
	Have you published the contact details of your DPO to facilitate your customers/employees in making contact with them?			
	Have you notified and published the contact details of the personal data protection officer and communicated them to the DPO?			
Data Protection Impact Assessments (DPIAs)	Is your data processing activity considered high-risk?			
Duplication of Records	If so, is there a process for identifying the need for, and conducting of DPIA's?			
	If you have carried out a DPIA, have you documented the procedure?			

DATA BREACHES

	Question	Yes	No	Comments/Remedial Action
Data Breaches	Does the organization have a documented privacy & security incident response plan? Are plans and procedures reviewed on a regular basis?			
	Is the reviewing process highlighted above documented?			
	Are procedures in place to notify the Data Protection & Privacy Office of a data breach?			

	Are there procedures in place to notify data subjects of a data breach if and when applicable?			
	Are all data breaches fully documented?			
	Are there cooperation procedures in place between data controllers, the suppliers and third parties to help resolve data breaches?			

STORAGE AND DATA TRANSFERS (OUTSIDE RWANDA) – *IF APPLICABLE*

	Question	Yes	No	Comments/Remedial Action
Access to personal data	Is personal data transferred outside the Rwanda?			
	Does the data transferred include any special categories of personal data?			
	Have you documented information about such transfers to include details of the nature of the data, the purpose of the processing, from/to which country the data is exported and who the recipient of the transfer is.			
	Is there a legal basis for the transfer?			
	Have you properly documented the legal basis for the transfer?			
	Are data subjects fully informed about any intended Data transfers of their personal data?			
	Is the transfer basing on the contract for transfer of personal data?			
	Do you have a valid authorization to share, transfer, and store personal data outside Rwanda?			

NOTE

This document is purely for guidance and does not constitute legal advice or legal analysis. All organizations that process personal data need to be aware that Law No 058/2021 of 13/10/2021 relating to the protection of personal data and privacy (DPP Law) will apply directly to them. The responsibility to become familiar with the DPP Law and comply with its provisions, therefore, lies with the organization. This guide is intended as a starting point only, and organizations may need to seek independent legal advice when reviewing or developing their own processes and procedures or dealing with specific legal issues or queries.