GUIDELINES ON DATA PROTECTION IMPACT ASSESSMENT (DPIA)

December 2023

TABLE OF CONTENTS

INTRODUCTION

Law No. 058/2021 of 13/10/2021 relating to the Protection of Personal Data and Privacy (DPP Law) establishes the comprehensive legal framework for protecting individuals' fundamental right to privacy and ensuring the responsible use of personal data in Rwanda. The risk-based approach and accountability principle embedded in the DPP Law requires data controllers and data processors to carry out a personal data protection impact assessment (DPIA), where the processing of personal data is likely to result in a high risk to the rights and freedoms of a natural person.

The National Cyber Security Authority (NCSA) through its Data Protection and Privacy Office has developed this document to guide data controllers and data processors through the process of determining whether their data processing operations require a DPIA and understanding when and how the DPIA should be carried out. This document provides a DPIA template inspired by compliance tools and best practices from different other data protection authorities across the globe.

WHAT IS A DPIA?

A DPIA is a process designed to describe the processing of personal data, assess its necessity and proportionality, and identify and mitigate the risks arising out of the processing. A DPIA does not have to indicate that all risks have been eradicated, but it should minimise the risks as far and as early as possible, and assess whether any residual risks are justified.

Along with minimising risks and demonstrating compliance with the DPP law, conducting a DPIA enables data controllers and processors to implement appropriate technical and organisational measures for data security, reduce operational costs, and incorporate 'data protection by design' into new data processing operations by optimising information flows and eliminating unnecessary data processing. Effective DPIAs help to build trust and confidence among citizens and partner organisations and carrying out DPIAs is the best practice and prudent to demonstrate compliance with the DPP Law.

WHAT DOES A DPIA ADDRESS? A SINGLE PROCESSING OPERATION OR A SET OF OPERATIONS?

An assessment usually concerns a single data processing operation. However, a single DPIA could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks.

In some circumstances, it may be reasonable and economical to conduct a single assessment, for example, where public authorities or several companies intend to establish a common online platform for data collection and service provision or similar technology (for example, an artificial intelligence (AI), facial recognition or video surveillance system) is used to collect the same type of data for the same purposes by different organisations.

WHEN IS THE DPIA CONDUCTED MANDATORY?

Under the DPP Law, a DPIA is mandatory where the processing of data **is likely to result in a high risk to the rights and freedoms of natural persons**.

A '**risk**' is a scenario describing an event and its consequences, estimated in terms of severity and likelihood. The risk in this context is about the potential for any significant physical, material or non-material harm to a natural person, e.g., where the processing is of such a nature that a personal data breach could jeopardise the physical health or safety of natural persons, or the processing gives rise to discrimination, exclusion, identity theft or fraud, financial loss, reputational damage, or any other significant economic or social disadvantage.

The reference to the '**rights and freedoms of natural persons**' concerns not only protection and respect of the right to privacy but also other rights and freedoms guaranteed by the Constitution of the Republic of Rwanda, including rights to equality, non-discrimination, inviolability, dignity, and integrity.

In addition to this general condition, Article 38 of the DPP Law further specifies that a DPIA is to be 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

Examples of such processing are screening employees and clients to comply with the AML/CFT[1] Law; tracking individuals' driving behaviour for offering insurance rates; genetic laboratories assessing and predicting disease/health risks; or any other processing operation that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract, e.g., a bank screening customer against a credit reference database to decide whether to offer them a mortgage.

The term '**systematic**' implies one or more of the following:

- ✓ occurring according to a system;
- ✓ pre-arranged, organised or methodical;
- ✓ taking place as part of a general plan for data collection;
- ✓ carried out as part of a strategy.

The term '**extensive**' should be interpreted as the processing of a wide range of data or affecting a large number of natural persons.

2. Processing of sensitive personal data on a large scale

To define what constitutes **large scale**, NCSA recommends considering the following factors:

- ✓ the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
- ✓ the volume of data and/or the range of different data items being processed;
- ✓ the duration, or permanence, of the data processing activity;
- ✓ the geographical extent of the processing activity.

[1] AML/CFT: Anti-money Laundering and Counter-terrorism Financing

The DPP Law defines **sensitive personal data** as 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.

Examples of large-scale processing of sensitive personal data may include a hospital (but not an individual doctor) processing patient data, a migration agency processing biometric data or police processing criminal records.

3. A systematic monitoring of a publicly accessible area on a large scale

The most apparent examples of systematic monitoring of a publicly accessible area on a large scale are video surveillance cameras, facial recognition systems or other data processing solutions used to observe, monitor or control a large number of data subjects. This type of monitoring is a criterion for a DPIA because personal data may be collected in circumstances where data subjects may not be aware of who is processing their personal data and how it will be used. Additionally, it may be impossible for individuals to avoid being subject to such monitoring in publicly accessible spaces, including streets, shopping malls, airports, convention centers, and banks.

In this context, the terms "systematic" and "large scale" refer not only to a large geographical coverage of the processing activity but also its duration or, the number or proportion of data subjects involved, the volume of personal data and/or the range of different personal data items being processed.

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

NCSA, identifies but not limited to the following processing operations as likely to result in a high risk to the rights and freedoms of natural persons:

1. **Processing data concerning vulnerable data subjects:** for example, children**,** people with disabilities, asylum seekers, refugees, the elderly, or in any case where a power imbalance in the relationship between the position of the data subject and the controller can be identified and where an individual may be unable to consent or oppose to the processing of his or her data.

2. **Matching or combining datasets:** for example, originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject. This is particularly relevant where personal data has not been obtained directly from data subjects, and transparency requirements are not met.

5. New technologies used to process personal data

Despite the immense potential to be used for the public good and contribute to sustainable development and economic growth, new technologies such as AI, market research involving neuro-measurement (i.e. emotional response analysis and brain activity), or the Internet of Things (IoT), depending on the specific circumstances of the processing, may involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. A DPIA will help the data controller and processors understand and manage such risks. Significant considerations should be given to societal implications and ethical concerns, such as the biases AI can embed, potentially resulting in discrimination, inequality, and exclusion.

In cases where it is not clear whether a DPIA is strictly mandatory, carrying out a DPIA is still the best practice and prudent to demonstrate compliance with the DPP Law.

WHEN SHOULD THE DPIA BE CONDUCTED?

The NCSA recommends carrying out a DPIA before the processing and as early as is feasible in the design of the processing operations. The NCSA urges data controllers and data processors to immediately carry out DPIAs for relevant processing operations.

As processing operations can evolve quickly and new vulnerabilities can arise, the DPIA should be considered as a living tool, not merely a one-off exercise. As a matter of good practice, a DPIA should be continuously and regularly re-assessed. Updating the DPIA will encourage finding privacy-friendly solutions and demonstrating compliance with the DPP Law.

A DPIA may also become necessary due to the change in the organisational or societal context of the processing operation, for example, if the effects of certain automated decisions have become more significant or new categories of data subjects become vulnerable to identity theft or fraud.

On the contrary, specific changes could lower the risk as well. For example, a processing operation could evolve so that decisions are no longer automated or a monitoring activity is no longer systematic. In that case, the review of the risk analysis can show that a DPIA's performance is no longer required.

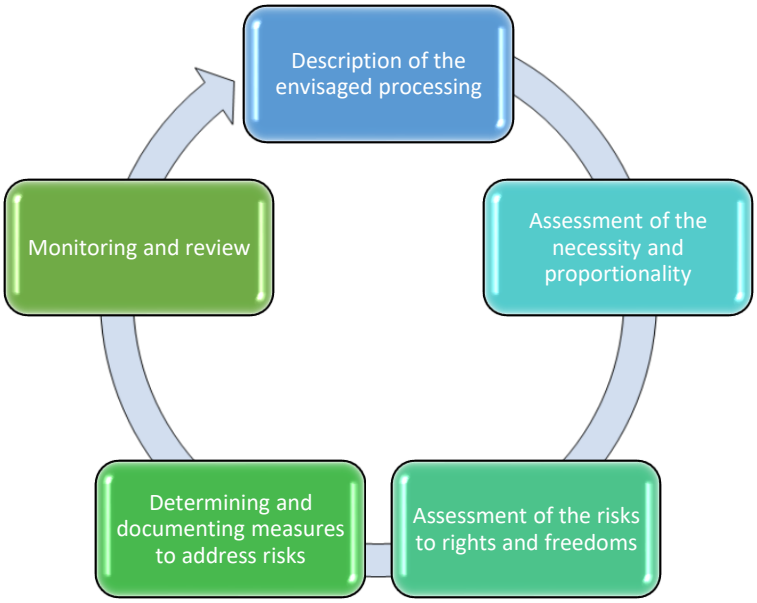
HOW TO CARRY OUT THE DPIA?

The following minimum features that should be present in a DPIA:

- ✓ A description of the envisaged processing operations and the purposes of the processing
- ✓ An assessment of the necessity and proportionality of the processing
- ✓ An assessment of the risks to the rights and freedoms of natural persons
- ✓ The measures envisaged to address the risks and demonstrate compliance with the law
- ✓ Monitoring and review.

This framework enables scalability and flexibility, so even small data controllers and data processors can carry out a DPIA and determine its precise structure and form.

The following figure illustrates the generic iterative process for carrying out a DPIA:



Step 1 - Description of the envisaged/existing[2] processing

Data controllers and data processors are required to describe the nature, scope, context, purposes, and legal grounds for processing personal data. In the case of complex processing operations, the NCSA recommends using a flowchart to illustrate the data flow to make the process easier to understand.

Step 2 - Assessment of the necessity and proportionality

For assessing and guaranteeing the proportionality and necessity of the processing, data controllers and data processors have to explain and justify the choices made to comply with the principles relating to the processing of personal data under Article 37 of the DPP Law. Necessity and proportionality should be considered in light of the specific circumstances of the processing operations. It must be assessed that there is a logical and direct link between the processing and the specified, explicit, and legitimate purpose(s) pursued by the data controller. It is necessary to evaluate the scope, extent, and intensity of processing as well as the quality of data and storage period in terms of the impact on fundamental rights, explaining with evidence why processing is strictly necessary, and other possible alternatives or less intrusive measures that are insufficient to reach the purposes sufficiently.

Step 3 - Assessment of the risks to rights and freedoms

Data controllers should list all risks as well as the potential impact on natural persons and any harm (physical, moral or material) that processing may cause e.g., loss of control over the use of personal data, discrimination, inability to exercise their rights (including but not limited to privacy rights); identity theft or fraud; financial loss; reputational damage; any other significant economic or social disadvantage. During the risk assessment process, it is crucial to consider the sensitivity of the personal data to be processed, the number of people likely to be affected and how they might be affected (starting from distress or inconvenience, to risks of financial loss or physical harm).

For each feared event (e.g., unauthorised access to a database; accidental loss of electronic equipment that may lead to the disclosure of personal data; cyber-attack; merging of datasets that

[2] For operations commenced before or during transitional period.

may result in processing more data about individuals than anticipated; data transfers to countries with inadequate data protection regimes), risk levels are to be defined considering two variables:

- **Severity**, which represents the magnitude of a risk. It primarily depends on the prejudicial nature of the potential impacts;
- **Likelihood,** which expresses the possibility of a risk occurring. It primarily depends on the level of vulnerabilities of the supporting assets when under threat and the level of capabilities of the risk sources to exploit them.

The 5x5 risk assessment matrix can be used. However, data controllers and data processors can apply 3x3 or 4X4 matrices that best suit existing risk assessment frameworks.

5X5 Risk Assessment Matrix Example						
Severity	Severe	Low to Medium	Medium	Medium to High	High	High
	Significant	Low	Low to Medium	Medium	Medium to High	High
	Moderate	Low	Low to Medium	Medium	Medium to High	High
	Minor	Low	Low	Low to Medium	Medium	Medium to High
	Negligible	Low	Low	Low	Low to Medium	Medium
		Very unlikely	Unlikely	Possible	Likely	Very likely
		Likelihood				

Recording sources against each risk identified will help to determine appropriate solutions, while the data flowchart generated during step 1 will help to identify weak spots, where general risks are likely to be particularly severe or give rise to specific risks.

Step 4 - Determining and documenting appropriate measures to address risks

First, the data controller or data processor should identify and describe measures and controls already applied, e.g., data protection policy and notices, protocols for managing incidents and breaches, encryption, anonymization, access control, backups, and hardware security. Based on the objective assessment process, it should be determined whether the risks identified can be considered acceptable given the existing controls. If not, additional measures should be introduced. There must be a solid justification for the proposed measures that could stand up to scrutiny.

In many cases, eliminating data protection risks completely will not be possible. Still, the aim is to reduce risks to a minimum and document those risks which have been accepted.

Mitigating measures could include but are not limited to refraining from collecting certain types of data; reducing retention periods; taking additional organisational and technical security measures; anonymising or pseudonymising data; training staff; due diligence in selecting third parties or offering clients the chance to opt out where appropriate.

It should be documented whether specific measures would reduce or eliminate the risks. Any decisions to accept data protection risks should be recorded. A data protection risk register could be a valuable tool as it enables one to go back to the register in case of any changes and note any steps taken to mitigate residual or emerging risks.

Keeping a record of all steps taken as part of the DPIA will help ensure that the process is completed thoroughly and enable the organization to demonstrate compliance with the DPP Law. Documentation also fosters the swift implementation of selected risk mitigation measures.

Step 5 - Monitoring and review

It is necessary to give effect to risk mitigation measures identified and make necessary adjustments in the processing operations. As part of the implementation of the DPIA, data controllers and data processors should keep data protection issues under review, and Data Protection Officers play an important role in this process. In particular, Data Protection Officers should assess whether the risk mitigation measures implemented have the intended effect of mitigating risks to the rights and freedoms of data subjects. Additionally, if there is a change in the risks represented by processing operations or the processing operations evolve or expand over time, it is necessary to assess

whether a further DPIA is required. A periodic review can also be built into the organisation's existing procedures.

WHO SHOULD BE INVOLVED IN CONDUCTING A DPIA?

The data controller is primarily responsible for ensuring the DPIA is carried out. If a data processor is involved in the processing, the data processor should assist with the DPIA and provide any necessary information.

The DPIAs should be mainly driven by people with appropriate expertise and knowledge of the processing operation(s) in question. The data controller or data processor may consider bringing in external specialists to consult on or to carry out the DPIA.

Under Article 41 of the DPP Law, any data controller or data processor must seek the advice of the Data Protection Officer when carrying out a DPIA. A Data Protection Officer should also monitor the performance of the DPIA.

As a matter of best practice, seeking the views of data subjects will allow the data controller to understand the worries of those who may be affected and to improve transparency by informing natural persons concerned about how their personal data will be used. The views of data subjects can be sought through various means, including surveys or focus group discussions. If the data controller's final decision differs from the viewpoints of data subjects, the reasons should be documented as a part of the DPIA.

WHEN SHALL THE SUPERVISORY AUTHORITY BE CONSULTED?

NCSA, as the supervisory authority, should be consulted:

- Where the data controller is not confident that processing operations are subject to a mandatory DPIA;
- Where the data controller is not certain that a single DPIA could be used to assess multiple processing operations;
- In case of any other doubts concerning the DPIA.

SHOULD THE DPIA BE PUBLISHED?

Publishing a DPIA is not a legal requirement. Still, making available a summary, conclusion, or even just a statement that a DPIA has been carried out would foster trust and demonstrate accountability and transparency.

The full DPIA must be communicated to the supervisory authority in case of consultation or if requested by the supervisory authority.

DPIA FORM

This form should be completed with reference to the DPIA guidelines provided above by the NCSA. It will help data controllers and, where applicable, data processors to assess the risks and document how decisions were made.

Data controller or Data processor name:	
Registration Number as a Data controller or Data processor	
Title of the project:	
Name and role of the person in charge of the project:	
Name of the Data Protection Officer:	
Name of the data processor(s), if involved:	
Name of the joint controller, if involved:	

The version history table below provides a history of the changes made to the document from its initial draft to the current version. The table below should be updated each time a significant change is made to the document.

Version	**Changes made**	**Approved by**	**Conducted by**	**Status**	**Date**
0.1				Draft	
1.0				Current version	

1. Description of the envisaged processing operations	
Purposes of processing: *Describe what the project aims to achieve, including where applicable, the legitimate interest pursued.*	
Categories of data subjects: (*e.g., children, employees, customers, patients, etc.)*	
An approximate number of natural persons and any vulnerable groups (children, people with disabilities, etc.) to be affected:	
Description of personal data: *(List elements of personal data to be processed concerning each category of data subject specified above, e.g., employees: name, address, email, etc.)*	
Processing operations: *(Select all envisaged)*	☐ Collection ☐ Recording ☐ Structuring ☐Storage ☐Adaptation ☐Retrieval ☐Reconstruction ☐Concealment ☐Consultation ☐Use ☐ Disclosure by transmission, sharing, transfer, or otherwise making available ☐ Sale ☐ Restriction ☐ Erasure or destruction

	☐ Other (specify) _____
The scope (extent, frequency, and geographic area) of the processing:	
The sources of data collection:	☐ Directly from data subjects ☐ Other sources In the case of other sources, list all 1. 2.
Grounds for processing personal data:	☐ Consent of data subject ☐ Contractual necessity ☐ Legal obligation ☐ Vital interests of the data subject or other person ☐ Public interest ☐ Performance of duties of public entity ☐ Legitimate interest ☐ Research upon authorization
Grounds for processing sensitive personal data:	☐ Consent of data subject ☐ Obligations of the data controller/ data processor or exercising specific rights of the data subject ☐ Vital interests of the data subject or other person ☐ Preventive or occupational medicine, public health ☐ Archiving, scientific and historical research or statistical purposes
Data would be stored:	☐ In Rwanda ☐ Outside Rwanda If outside Rwanda, here is a list of countries and hosting service providers: 1. 2. Reasoning for storing personal data outside Rwanda:

Data would be shared/transferred:	☐ In Rwanda ☐ Outside Rwanda If outside Rwanda, here is a list of countries and recipients' names: 1. 2. Purposes for transferred personal data outside Rwanda:
Retention periods envisaged for each category/type of data:	
DPIA is required due to:	☐ 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 ☐ Processing of sensitive personal data on a large scale ☐ A systematic monitoring of a publicly accessible area on a large scale ☐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 ☐ New technologies used to process personal data

2. Assessment of the necessity and proportionality	
Legal grounds for processing:	☐ Consent of data subject ☐ Contractual necessity ☐ Legal obligation ☐ Vital interests of the data subject or other person ☐ Public interest ☐ Performance of duties of public entity ☐ Legitimate interest ☐ Research upon authorization ☐ Necessity for purposes of preventive or occupational medicine, public health ☐ Necessity for archiving purposes in the public interest scientific, historical research or statistical purposes.
Justification of necessity: *Describe why achieving the same outcomes is impossible through other means or less data.*	
Justification of proportionality: *Describe how you ensure data minimization, quality of data, appropriateness of security measures, and data subject rights.*	

3. Risk assessment							
Risk	Source of the risk	Potential impact on individuals	Risk assessment			Current Measures/ controls	Risk owner
			Severity	Likelihood	Overall level		

4. Risk mitigation (applicable only to medium or high risks under section 4)					
Risk	Suggested corrective measures /controls	Effect on risk (Eliminated, reduced or accepted)	Residual risks	Measures/controls approved (yes/no)	Risk owner