National Cyber Security Authority

DPO

Data Protection and Privacy Office

GUIDE ON CONTRACTUAL PROVISIONS FOR PROCESSING OF PERSONAL DATA

www.dpo.gov.rw

dpp@dpo.gov.rw

9080

April 2024

TABLE OF CONTENTS

GUIDE ON CONTRACTUAL PROVISIONS FOR PROCESSING OF PERSONAL DATA

INTRODUCTION

Following the passing of Law Nº 058/2021 of 13/10/2021 relating to the protection of personal data and privacy (hereafter referred to as the "DPP Law"), which applies to processing performed on personal data or on sets of personal data whether or not by automated means, such as accessing, obtaining, collecting, recording, structuring, storing, adapting or altering, retrieving, reconstructing, concealing, consulting, using, disclosing by transmission, sharing, transfering, or otherwise making available, selling, restricting, erasing or destroying personal data as provided for in Article 3 (point 4).

Among the provisions of the DPP Law, Article 4 specifically makes it mandatory for every Data Controller whose processing operation(s) involves a Data Processor, to govern such involvement by a written contract known as a data processing agreement. In other words, when a Data Controller engages a Data Processor to process personal data on its behalf, the Data Controller and Data Processor must enter into a legally binding written contract governing this processing of personal data. This obligation is relevant to Data Controllers and Data Processors in both the public and private sectors.

Moreover, according to Article 4 of the DPP Law, the Data Controller should authorise and enter into a data processing agreement with the Data Processor, who provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing of personal data meets the requirements of the DPP Law. Some examples of the considerations Data Controllers should have when assessing whether the Data Processor provides "sufficient guarantees" could include but are not limited to providing the Data Controller with relevant documentation, e.g. their privacy policy, record management policy, and information security policy. Whether the guarantees are sufficient depends on both the processing circumstances and the risk posed to the rights of data subjects.

Nevertheless, the data processing agreement is not limited to Data Controller to Data Processor relationships. The data processing agreement also covers other relationships mentioned in the DPP Law, such as Data Controller to Data Controller (including joint controllership), Data Controller to a third party, and Data Processor to a third party.

Furthermore, the contract law provides for the will of parties to enter into an agreement; this guide outlines mandatory provisions that parties must adhere to in their processing operations for personal data. Thus, the parties are free to incorporate other provisions that illustrate their processing operations in respect to the DPP Law.

WHEN IS THE DATA PROCESSING AGREEMENT NEEDED?

It is common practice for Data Controllers to take advantage of the Data Processor's expertise and experience in a particular processing operation and engage them in processing personal data on their behalf. For example:

- Many organisations use cloud services to store the data they collect securely. In this case, organisations are the Data Controller and the cloud service providers act as their Data Processors.
- When a marketing company sends promotional emails and vouchers to customers on the store's behalf, the marketing company is the Data Processor and the store is the Data Controller.
- When a factory uses a payroll company's services and IT system to pay wages, the factory is the Data Controller, and the payroll company is the Data Processor.

In all of the cases mentioned above, a Data Controller who engages a Data Processor to process personal data, there must be a written contract that binds the Data Processor to the Data Controller with respect to the processing activities.

For Data Controllers, Data Processors and third parties whose processing operations involve delegation of responsibilities must enter into a data processing agreement laying out responsibilities that involved parties are going to have while processing personal data, and technical and organisational measures in place in regards to how personal data is stored, transferred, altered, processed, accessed, and used. This agreement also defines the limits within which the Data Controllers, Data Processors and third parties are going to process personal data.

MANDATORY PROVISIONS TO BE INCORPORATED IN THE DATA PROCESSING AGREEMENT

A data processing agreement must include, at a minimum, the following provisions:

- The scope and purpose of processing personal data;
- The type of personal data being processed;
- The categories of data subjects whose personal data is being processed;
- A description of each type of personal data included within each category of personal data;
- Obligations of the Data Controller;
- Obligations of the Data Processor;
- Obligations of the Third Party;
- Technical and organizational measures to ensure the security of personal data;
- Data subjects' rights;
- The duration of the retention period for the data being processed;
- Reference that the governing law is the DPP Law;
- Choice of forum;
- Redress;
- Liability;
- End-of-contract provisions.

The contract should also contain the following mandatory conditions:

- The Data Processor will only process personal data received from the Data Controller on documented instructions of the Data Controller, including with respect to storing, sharing or transferring personal data outside Rwanda;
- The Data Processor ensures that any person(s) processing personal data is subject to a duty of confidentiality;
- The Processor takes all measures to ensure the security of the personal data in accordance with Article 47 of the DPP Law;
- That the Data Processor obtains prior authorisation for any third party the Data Processor may engage to process the personal data received from the Data Controller; And that any third party engaged by the Data Processor are subject to the same data

protection obligations as the Data Processor that remains directly liable to the Data Controller for the performance of a third party's data protection obligations;

- The Data Processor assists the Data Controller in responding to data subject requests to exercise their rights;
- The Data Processor assists the Data Controller to ensure compliance with obligations under the DPP Law, including notification of data breaches and data protection impact assessments;
- At the end of the data processing by the Data Processor and on the Data Controller's instruction, the Data Processor deletes or returns the personal data received from the Data Controller;
- The Data Processor makes available to the Data Controller all information necessary to demonstrate compliance with DPP law.

HOW TO ENSURE COMPLIANCE WITH THE DPP LAW?

For any natural person, public or private corporate body or legal entity who engages a Data Controller, Data Processor or third party has the obligation to ensure that such processing operation is bound by a data processing agreement which is up to date and fully compliant with the DPP Law, and that the agreement contains, at a minimum, the mandatory provisions which are prescribed in this guide.

CONCLUSION

Parties to the data processing agreement should be mindful that there are a number of other obligations which the DPP Law imposes, such as record keeping, data logging, and ensuring the security of personal data, amongst others.

These direct obligations of the DPP Law apply to Data Controllers, Data Processors and third parties without prejudice to other contractual provisions of the data processing agreement to which parties will be subject.