National Cyber Security Authority

DPO DATA PROTECTION OFFICE

GUIDANCE NOTE ON DESIGNATION OF THE DATA PROTECTION OFFICER (DPO)

www.dpo.gov.rw

dpp@dpo.gov.rw

9080

TABLE OF CONTENTS

1. Who is a Data Protection Officer (DPO)? 2
2. Mandatory designation 2
3. Can entities appoint a DPO jointly? If so, under what conditions? 2
4. Where should the DPO be located? 2
5. Can the Data Protection Officer be an existing employee? 3
6. Can we contract out the role of the Data Protection Officer? 3
7. Qualifications of the Data Protection Officer 3
8. Duties of the Data Protection Officer 4
   - To inform and advise the data controller or data processor 4
   - Compliance with DPP Law and with the policies of the data controller or data processor in relation to the protection of personal data 4
   - To provide advice in regards to Data Protection Impact Assessment 4
   - To cooperate with the Supervisory Authority 4
9. What resources should be provided to the DPO by the data controller or data processor? 5
10. Is the DPO personally responsible for non-compliance with data protection requirements? 5

GUIDANCE NOTE ON DESIGNATION OF THE DATA PROTECTION OFFICER (DPO)

1. Who is a Data Protection Officer (DPO)?

A Data Protection Officer (DPO) is a person who oversees the implementation and enforcement of data protection and privacy measures for a given entity.

2. Mandatory designation

The data controller and the data processor designate a data protection officer where:

i. the processing of personal data is carried out by public or private corporate body or a legal entity, except courts.
ii. the core activities of the data controller or the data processor consist of personal data processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale.
iii. the core activities of the data controller or the data processor consist of processing on a large scale of special categories of data.

The DPO will be the contact point with respect to data subjects, the supervisory authority[1] and internally within the organization.

3. Can entities appoint a DPO jointly? If so, under what conditions?

A group of undertakings may appoint a single personal data protection officer provided that the data protection officer is easily accessible from each establishment.

Where the data controller or the data processor is a public authority or body, a single personal data protection officer may be designated for several such authorities or bodies, taking account of their organizational structure and size.

Entities are also required to establish an internal compliance team that shall work under the direct supervision of the appointed data protection officer to ensure the protection of personal data and privacy in their respective entities.

4. Where should the DPO be located?

To ensure that the DPO is accessible, it is recommended that the DPO is located in Rwanda when a data controller or the data processor is established in Rwanda. However, it cannot be excluded that, in some situations where the data controller or the data processor has no establishment in

[1] Supervisory authority: National Cyber Security Authority (NCSA)

Rwanda, a DPO may be able to carry out his or her activities in collaboration with representative in Rwanda.

5. Can the Data Protection Officer be an existing employee?

The data protection officer is designated on the basis of professional qualities, expert knowledge of personal data protection, practices and the ability to fulfil the tasks assigned to him or her.

Should these qualities be of an existing employee, the DPO should not be expected to manage competing objectives that could result in data protection taking a secondary role to business interests.

6. Can we contract out the role of the Data Protection Officer?

The personal data protection officer may be a permanent staff member of the data controller or the data processor, or a person who fulfils the tasks on the basis of a service contract.

The data controller or the data processor must publish the contact details of the personal data protection officer and communicate them to the supervisory authority.

7. Qualifications of the Data Protection Officer

The DPO shall be designated on the basis of professional qualities and, in particular, knowledge of data protection and privacy laws and practices and the ability to fulfil his or her tasks.

A data protection officer is expected to have the following skills:

- Knowledge of the business sector and his/her entity
- Knowledge in national data protection laws and practices
- Understanding of the processing operations carried out by his/her entity and risks involved Knowledgeable understanding of information technologies and data security for both digital data and manual data
- Ability to train his/her colleagues and promote a data protection and privacy culture within the entity

The personal data protection officer must in the performance of his or her tasks have due regard to the risk associated with personal data processing operations, considering the nature, scope, context and purpose of processing.

The DPO's main concern should be enabling compliance with the Law relating to the protection of personal data and privacy (hereafter "DPP Law"). Therefore, DPO should be chosen cautiously with regard to the data protection issues that arise within the entity.

8. Duties of the Data Protection Officer

The personal data protection officer has the following duties:

- **To inform and advise the data controller or data processor**

The DPO has the duty to inform and advise the data controller or data processor and the employees who carry out personal data processing, of their obligations pursuant to the DPP Law.

- **Compliance with DPP Law and with the policies of the data controller or data processor in relation to the protection of personal data**

The DPO to ensure compliance shall:

i. collect information to identify processing activities;
ii. analyze and check the compliance of processing activities;
iii. inform, advise and issue recommendations to the data controller or data processor;
iv. to monitor in his or her area of work the assignment of responsibilities;
v. conduct awareness-raising and training of staff involved in personal data processing operations, and
vi. perform related audits.

- **To provide advice in regards to Data Protection Impact Assessment**

As far as the data protection impact assessment (DPIA) is concerned, the DPO monitors its performance on the following issues, amongst others:

i. whether or not to carry out a DPIA;
ii. what methodology to follow when carrying out a DPIA;
iii. whether to carry out the DPIA in-house or whether to outsource it;
iv. what safeguards (including technical and organizational measures) to apply to mitigate any risks to the rights and interests of the data subjects;
v. whether or not the DPIA has been correctly carried out and whether its conclusions are in compliance with DPP Law.

- **To cooperate with the Supervisory Authority**

The DPO shall act as the contact point on issues relating to processing of personal data, including the prior consultation and to consult, where appropriate, with regard to any other matter the Supervisory Authority.

9. What resources should be provided to the DPO by the data controller or data processor?

The Data Protection Officer must have the resources necessary to be able to carry out his or her tasks. Depending on the nature of the processing operations and the activities and size of the entity, the following resources must be provided to the Data Protection Officer:

- active support of the Data Protection Officer's functions by senior management;
- adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and additional staff where appropriate;
- official communication of the designation of the Data Protection Officer to all staff members;
- access to other services within the entity so that Data Protection Officer(s) can receive essential support, input or information;
- continuous access to trainings.

10. Is the DPO personally responsible for non-compliance with data protection requirements?

DPOs are not personally responsible for non-compliance with data protection requirements. It is the data controller or data processor who is required to ensure and be able to demonstrate that processing is performed in accordance with the DPP Law.

Data protection compliance is the responsibility of the data controller or data processor. Therefore, even though the data protection officer is responsible for assisting the data controller or data processor in monitoring the internal compliance, the data protection officer is not personally responsible for any non-compliance with the DPP Law by the data controller or data processor.

NOTE

This document is purely for guidance and does not constitute legal advice or legal analysis. All entities 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 entity.

This guide is intended as a starting point only, and entities may need to seek independent legal advice when reviewing or developing their own processes and procedures or dealing with specific legal issues or queries