| | |
|---|---|
| **Ref. No.:** | **[Sub. D. 74:05]** |
| **Draft:** | **Data Protection (Reasonable Measures for Engaging Data Processors) Rules, 2022**<br>**(Subject to Change)** |
| **Author:** | **Macmillan Keck, Attorneys & Solicitors**<br>**Attorneys, Consultants** |
| **Date:** | **Draft – ~~22~~ ~~July~~ 5 September 2022** |

**DRAFT**

# DATA PROTECTION (REASONABLE MEASURES FOR ENGAGING DATA PROCESSORS) RULES, 2022

# DATA PROTECTION (REASONABLE MEASURES FOR ENGAGING DATA PROCESSORS) RULES, 2022

Government Notice No.: …… of 2022

[DATA PROTECTION ACT, 2022]

(Cap.[74:05])

DATA PROTECTION (REASONABLE MEASURES FOR ENGAGING DATA PROCESSORS) RULES, 2022

*under ss 12 and 25*

IN EXERCISE of the powers conferred by sections 12 and 25 of the [Data Protection Act, 2022], the Authority makes the following Rules —

Citation

**1.** These Rules may be cited as the Data Protection (Reasonable Measures for Engaging Data Processors) Rules, 2022.

Interpretation

**2.** In these Rules, unless the context otherwise requires—

"engaging entity" means a data controller or data processor that engages a data processor to process personal data on its behalf or at its direction.

Scope of rules

**3.** These Rules shall provide for reasonable measures that an engaging entity must take when engaging a data processor in order to satisfy the requirements of section 25 of the Act.

Obligations of a data controller or data processor engaging a data processor

**4.** (1) Pursuant to section 25(1) of the Act, where an engaging entity engages the services of a data processor, the engaging entity shall take reasonable measures to ensure that the data processor shall—

(a) comply with the principles and obligations in section 23 of the Act applicable to the data controller in relation to the collection, further processing and retention of personal data and requirements that the personal data be adequate, relevant, limited, accurate, complete, not misleading and up-to-date;

(b) assist the engaging entity by appropriate technical and organizational measures, where practical, in the fulfilment of the

data controller's obligations to honour the individual rights of data subjects under Part IV of the Act;

(c) implement appropriate technical and organizational measures to ensure the security, integrity and confidentiality of personal data in its possession or under its control as required in Part V of the Act, with due regard to section 32 of the Act;

(d) provide the engaging entity with any information it reasonably requires to comply and demonstrate compliance with the Act; and

(e) notify the engaging entity of the proposed engagement of any new data processor, and comply with the engaging entity's reasonable objection or instruction in relation thereto.

(2) If a data processor receives a notification under subrule (1)(e) from another data processor which it has in turn engaged, the former shall:

(a) notify the engaging entity that engaged it of the notification it has received; and

(b) comply with such engaging entity's reasonable objection or instruction in relation thereto.

(3) Subject to subrule (4), any notification of the proposed engagement of any new data processor under subrule (1)(e) or (2) of this rule shall be made sufficiently early and in such manner as to allow the recipient of the notification a reasonable opportunity to review and object to or provide instructions in relation to such engagement.

(4) If it is not feasible for a data processor to comply with subrule (3), the notification shall when made provide a detailed account of the reasons therefor.

Written agreement with a data processor

**5.** (1) Subject to rule 6, an engaging entity shall be presumed to have engaged in "reasonable measures" for the purposes of rule 4 if it enters into written agreement with the data processor—

(a) setting out the nature, purpose and duration of the processing to be performed by the data processor;

(b) setting out the likely categories of data subjects and types of personal data to be processed by the data processor, separately noting any types of sensitive personal data likely to be processed;

(c) requiring that personal data only be processed by the data processor upon written instructions of the engaging entity, unless otherwise required by applicable law;

(d) requiring that personal data only be transferred from Malawi to another country by the data processor upon written instructions of the engaging entity and in compliance with Part IV of the Act;

(e) requiring the data processor to assist the engaging entity, by appropriate technical and organizational measures, where practical, in fulfilling the engaging entity's statutory or contractual obligations relating to section 23 of the Act with respect to the collection, further processing and retention of personal data and requirements that the personal data be adequate, relevant, limited, accurate, complete, not misleading and up-to-date;

(f) requiring the data processor to assist the engaging entity, by appropriate technical and organizational measures, where practical, in connection with a data protection impact assessment relating to section 24 of the Act;

(g) requiring the data processor to assist the engaging entity, by appropriate technical and organizational measures, where practical, in fulfilling the engaging entity's statutory or contractual obligations relating to the rights of data subjects under Part VI of the Act;

(h) requiring the data processor to have implemented, prior to commencing any processing, the technical and organizational measures necessary to—

i. ensure the security, integrity and confidentiality of personal data in its possession or under its control in accordance with section 31 of the Act; and

ii. make the data breach notifications in accordance with section 33 of the Act.

(i) requiring the data processor to provide the engaging entity with any information it reasonably requires to comply and demonstrate compliance with the Act or, where the engaging entity is also a data processor, with the terms and conditions on which such data processor was engaged;

(j) requiring the data processor to provide access to the engaging entity, or a representative thereof, to conduct reasonable audits and inspections to confirm compliance with the agreement and the Act;

(k) setting out any data processors it has engaged that would process the personal data on its behalf;

(l) requiring the data processor to notify the engaging entity when it engages any new data processor, in compliance with the requirements of these rules;

(m) requiring the data processor to delete or return to the engaging entity all personal data in its possession or control when the engagement is terminated or the stated duration of the processing has otherwise come to an end;

(n) requiring the data processor to undertake that any other data processor it has engaged or engages will be bound by substantially the same data protection obligations as those applicable to it; and

(o) making the data processor fully responsible to the engaging entity for the performance by any other data processor the former has engaged and requiring the former to notify the engaging entity of any failure by such other data processor to fulfil its contractual obligations or its obligations under the Act.

(2) The standard contractual clauses set out in Schedule 1 may be used by data controllers and data processors to establish a written agreement in accordance with subrule (1).

(3) Notwithstanding subrule (2)—

(a) the standard contractual clauses may be modified to align with the specific circumstances of the engagement or the anticipated processing of personal data;

(b) if any such modification weakens, limits or eliminates the protections established in the standard contractual clauses set out in Schedule 1, such modified contractual clauses may not fulfil the requirements of subrule (1); and

(c) data controllers and data processors must use their reasonable judgment to determine whether additional contractual provisions are required satisfy section 25(1) of the Act in order to address the particular circumstances of an engagement or the anticipated processing of personal data.

(4) Subject to rule 6, when considering "reasonable measures" for the purposes of section 25(1) of the Act and rule 4, an engaging entity may take into account the data processor's legally binding commitment or adherence to binding corporate rules, codes of conduct or certification mechanisms that afford the necessary protections.

Diligence when engaging a data processor

**6.** (1) An engaging entity shall not satisfy the "reasonable measures" requirement in section 25(1) of the Act and rule 4 unless it conducts reasonable diligence on the data processor it engages.

(2) Reasonable diligence under subrule (1) includes assessment, at the time of engagement of the data processor and from time to time thereafter, of the technical, organizational, financial and other relevant capabilities of the data processor and its ability to comply with the Act and any written agreement between the engaging entity and data processor, and any relevant binding corporate rules, codes of conduct or certification mechanisms relied upon by the data processor.

## SCHEDULE 1 – Standard contractual clauses

**1. Description of the processing**

The details of the processing to be performed by [*data processor to be engaged*] on behalf of the [*data controller/data processor engaging*], are specified in [*Annex I*] to this Agreement.

**Written instructions for processing and international transfers**

(1) The [*data processor to be engaged*] shall process personal data only on, and only to the extent set out in, written instructions from the [*data controller/data processor engaging*], except to the extent such processing is required by applicable law.

(2) Without limiting the preceding paragraph, the [*data processor to be engaged*] shall only transfer from Malawi to another country upon written documented instructions from the [*data controller/data processor engaging*] and in compliance with Part VI of the Act.

**Assistance to the [*data controller/data processor engaging data processor*]**

(1) The [*data processor to be engaged*] shall provide assistance to the [*data controller/data processor engaging*] by appropriate technical and organizational measures, where practical, in:

(a) [fulfilling its obligations under section 23 of the Act / fulfilling its contractual obligations to assist the data processor or data controller that has engaged it relating to section 23 of the Act];

(b) [conducting a data protection impact assessment under section 24 of the Act / fulfilling its contractual obligations to assist the data processor or data controller that has engaged relating to a data protection impact assessment under section 24 of the Act];

(c) [fulfilling its obligations to data subjects under Part IV of the Act / fulfilling its contractual obligations to assist the data processor or data controller that has engaged it relating to Part IV of the Act];

(2) The [*data processor to be engaged*] shall promptly notify the [*data controller/data processor engaging*] of any request it has received from the data subject and shall not respond to the request itself, unless authorized or instructed in writing to do so by the [*data controller/data processor engaging it*].

**Data security measures**

The [*data processor to be engaged*] shall have implemented, prior to commencing any processing, the technical and organizational measures necessary to:

(a) ensure the security, integrity and confidentiality of personal data in its possession or under its control as required be section 31 of the Act; and

(b) make the data breach notifications to the [*data controller/data processor engaging*] required by section 33 of the Act.

**Documentation and compliance**

(1) The [*data processor to be engaged*] shall maintain adequate records to demonstrate compliance with this Agreement and its obligations under the Act.

(2) The [*data processor to be engaged*] shall retain copies of any written instructions it receives from the [*data controller/data processor engaging*] relating to the processing to by undertaken this Agreement.

(3) The [*data processor to be engaged*] shall immediately notify the [*data controller/data processor engaging*] in writing if it reasonably believes any such instructions would violate the Act or this Agreement and the [*data processor to be engaged*] shall retain copies of any such notification.

(4) The [*data processor to be engaged*] shall provide access to the [*data controller/data processor engaging*], or a representative thereof, to conduct reasonable audits and inspections to confirm compliance with the agreement and the Act.

**Engagement of a data processor**

(1) The [*data processor to be engaged*] has engaged the data processors set out in Annex I that will process personal data that is the subject of this Agreement on its behalf and has set out any data processors further engaged by those data processors.

(2) The [*data processor to be engaged*] will notify the [*data controller/data processor engaging*] in writing if it:

(a) will engage the services of another data processor not listed in Annex I to process the personal data that is the subject of this agreement; or

(b) receives a similar notification from any data processor engaged by it.

(3) The notification to the [*data controller/data processor engaging*]:

(a) must be made prior to any such engagement to allow sufficient time for the [*data controller/data processor engaging it*] to review and object to such engagement; or

(b) if such prior notification is not feasible, provide a detailed account of the reasons therefor with the notification.

(4) The [*data processor to be engaged*] undertakes that any data processor it has engaged or engages with respect to processing personal data that is the subject of this Agreement will be bound by substantially the same data protection obligations as those applicable to [*data processor to be engaged*] hereunder.

(5) The [*data processor to be engaged*] will remain fully responsible to the [*data controller/data processor engaging*] for the performance of the obligations of any data processor that the [*data processor to be engaged*] may engage, and [*data processor to be engaged*] will notify the [*data controller/data processor engaging*] of any failure by such data processor to fulfil such obligations.

**Termination or completion of processing**

Unless otherwise instructed in writing by the [*data controller/data processor engaging*], the [*data processor to be engaged*] shall [delete / return to the [*data controller/data processor engaging it*]] the personal data processed under this Agreement:

(a) upon the termination of the engagement under this Agreement; or

(b) when the stated duration of the processing of such personal data has otherwise come to an end.

## ANNEX I to standard contractual clauses

1. **Nature, purpose and duration of the processing**

   [*Provide a description of the nature and purpose of the processing by the data processor and the anticipated duration of the processing.*]

   **Categories of data subjects**

   [*Provide a description of the categories of data subjects whose personal data is likely to be processed by the data controller.*]

   **Types of personal data to be processed**

   [*Provide a description of the types of personal data that are likely to be processed, separately noting any types of personal sensitive personal data that are likely to be processed.*]

   **Data processors engaged**

   [*Provide a list of all engaged data processors that will process data that are the subject of this Agreement on behalf of the data processor to be engaged by this Agreement. For each listed data processor, list any data processors that it has, in turn, engaged, and so forth down the chain of data processors. For each data processor listed, include name, address, contact person and contact details.*]