STAKEHOLDER CONSULTATION REPORT

FOR

PHASE 2

OF

PROVISION OF LEGAL CONSULTANCY SERVICES TO PRODUCE DATA PROTECTION LEGISLATION FOR THE GOVERNMENT OF MALAWI

REF NO.: MW-PPPC-62396-CS-QCBS
Project No: P16053

Submitted by:

MACMILLAN KECK
ATTORNEYS & SOLICITORS

5 September 2022

Contents

Introduction

In this Stakeholder Consultation Report, we summarise the 2-day stakeholder consultation meetings conducted on July 26-27, 2022 in Malawi and remotely. We presented five pieces of secondary legislation, which will be adopted based on the powers that the Act confer on the Authority once it enters into force.

We have also received written feedback after the conclusion of the stakeholder consultation meetings. This report captures how we have responded to the feedback and explains the changes that were made in the rules based on the feedback received.

Planning and agenda

The rules that were prepared under Phase 2 were presented remotely. A conference room was set up at MACRA's premises with videoconferencing capabilities. The stakeholders were given the option to join remotely or physically. Two 3-hour sessions were scheduled on two consecutive days.

The agenda for the meetings was as follows:

DAY 1:26 JULY 2022

13h00 Introductions

13h10 Welcoming Remarks

13h20 Keynote address by Ministry of Information and Digitalization

13h30 Remarks by the Consultants MacMillan Keck

PRESENTATIONS OF THE REGULATIONS: -

13h40 Guideline and checklist on compliance

14h20 Discussions, Questions and Answers

HEALTH BREAK

13h00 Rules on registration and Annual fees

13h40 Discussions, Questions and Answers

15h00 Rules on reasonable measures for engaging a data processor

15h40 Discussions, Questions and Answers

END OF DAY ONE

DAY 2:27 JULY 2022

Recap on yesterday's Presentations & Discussions

Presentation on regulations, Cont'd….

15h20 Guidelines on data breach notifications

16h00 Discussions, Questions and Answers

14h20 Rules of complaints and investigations

HEALTH BREAK

15h00 Discussions, Questions and Answers

15h40 Project Road map

16h00 Closing Remarks by MACRA

16h20 End of the Meeting

Participants

The following participants attended the stakeholder consultations:

Chimwemwe Matemba, MACRA

Bram Fudzulani

Michael Bakaimani, ICT Association of Malawi - Member, mbakaimani@gmail.com

Loveness Phale, CDH Investment Bank

Vincent Jere, Telekom Networks Malawi Plc

Gregory Kachale, Research Bureau International, gregk@researchbi.com

Loveness Phale, CDH Investment Bank, lphale@cdh-malawi.com

Lloyd Momba, MultiChoice, Lloyd.Momba@multichoice.co.za

Allan Banda, Airtel Malawi, allan.banda@mw.airtel.com

Leona Mkandawire, Old Mutual, lmkandawire@oldmutual.co.mw

Ritu Kumar Mishra, UNDP

Gerald Chungu, Old Mutual, gchungu@oldmutual.co.mw

Chimwemwe Kadangwe, Old Mutual Malawi, ckadangwe@oldmutual.co.mw

Vincent Jere, Telekom Networks Malawi Plc, vincent.jere@tnm.co.mw

Felizarda Mbewe, Old Mutual Malawi,

Salome Mdala, Reunion Insurance Company, smdala@reunioninsurance.com

Felizarda Mbewe, Old Mutual Malawi, fmbewe@oldmutual.co.mw

Sandra Moto, Old Mutual, smoto@oldmutual.co.mw

Lusungu Mkandawire, Ecobank, lmkandawire@ecobank.com

Chisomo Bekete Unitrans Africa and ICTAM Member, chisomo.bekete@unitrans.afrca

Maya Biziwick, CDH Investment Bank, mbiziwick@cdh-malawi.com

Christopher Chibwana, MultiChoice, Christopher.Chibwana@mw.MultiChoice.com

Rory Macmillan, Jason Blechman and Lale Tuzmen of Macmillan Keck Attorneys & Solicitors (the consultants)

Discussions and feedback

Day 1

On the first day, Rory Macmillan presented Guideline and Checklist on Compliance and Rules on Registration and Annual Fees. Jason Blechman presented Rules on Reasonable Measures for Engaging a Data Processor.

The following topics were discussed during the first day of consultations:

- **Data processors and data controllers of major importance**
    - We received a question on what it means to be a data processor or data controller of major importance, which we explained by sharing the definition in the regulations.

- We received a question on the two-year grace period for local companies. We confirmed that data processors and data controllers that are in Malawi and are not data processors or data controllers of major importance are exempt for the first two years.
- There was a question on the origin of the 10,000 number of data subjects used to define data controllers and processors of major importance. We explained the process, different countries' approaches and judgement calls used leading to propose this number.
- We received a question on how to count individuals happens if a data subject is cited in connection with multiple uses of a single product. For example, if an individual is registered twice for different products, is the individual counted twice? We clarified that one individual is only counted once.
- With respect to the Rules on Registration and Annual Fees, there was a question on what constitutes a significant change to be notified to the Authority. We explained that the significance of a change to an organization's data processing is context-dependent and offered examples. For example, if an organization was not processing "sensitive data" but then began processing large volumes of data including health data, that sort of shift could be a significant change. Also, a change to the organisation's tier of turnover for purposes of calculating annual fees would have to be notified.

- **Consent**
  - There were some questions on whether there is requirement that consent be in a language the data subject will understand. For example, what happens if the data subject does not understand English? We explained that consent must be informed, so notification would have to be explained to the data subject in a language that they understand.
  - We received a question on whether consent required for CCTV in public places. In this case, the Act's provisions on lawful basis for processing would apply.
  - A question was raised relating to employees giving consent in their employment contracts, and whether consent might be bundled into an employment contract. We explained that broad consent provisions are not permitted – the data minimisation and other principles of the bill will apply, so consent to process all of an employee's personal data should not be a condition in an employment contract. It is important for employee to be informed which data are being collected and why. For example, bank account information would be needed for payment of the employee's salary.

- **Data breach notifications**
  - There was a question on how to distinguish high risk and low risk harm to rights and freedoms of data subjects. We explained by giving examples that illustrated high risk. These are very much context-specific determinations. The Authority will be working with organizations in Malawi to help them consider which risks should be viewed as high or not. The two-year grace period will allow for this process to happen before all provisions of the Act enter into force.

- There was a question on period of time to notify the data subject if there is a high-risk breach. The deadline of "undue delay" to notify a data subject was discussed and clarified.
- We received a question on why the deadline for breach notifications is 72 hours while the GDPR requires 48 hours. It was discussed that preparing a notification involves an extensive amount of work, and this would be done under extreme pressure of time. The organisations in Malawi may not have the same resources as are available to European organisations to complete everything within 48 hours.
- Within the framework of data breaches, there was a question on how using personal email addresses is handled elsewhere, such as where the data goes and how it is handled if there are leaks. Section 31 of the bill addresses data security. Data processors have to implement data security measures. Section 32 includes some guidelines on how to think about data security. Each data controller and data processor would have to verify that the data they are processing is adequately protected.

- **Extra-terrestrial application**
  - We received a question on how organisations processing data outside of Malawi, such as Visa and Mastercard, will be impacted. We explained that the act applies to organisations outside of Malawi that are targeting Malawi for their services and are using data about people in Malawi.
- **Alignment with AU policy**
  - Stakeholders highlighted that the regulations and the bill come at a time when the AU released a data policy framework.
  - On data portability, we explained that the law provides the Authority the option to trigger the data portability right. It does not apply right away. The reason is that data portability is quite costly for organisations to implement. It will require setting up technical protocols to prepare for it technically. There should be an assessment whether the cost is worth the benefit. Data ideally should be portable, but this is context-specific and requires a detailed analysis before making the investment. Our view is that simply allowing data portability rights to all data subjects is excessive without proper examination to justify it.
  - On cross-border data flows and collaboration on the continent while protecting rights, we shared our active involvement in this field.
- **The Bill**
  - We also received several questions about the bill.
  - There was a discussion on the sequence of adoption of these rules and regulations. We explained that the bill would be adopted first and then the Authority would adopt these rules under the act. If there are amendments to the bill, they will have to trickle down to the rules and may require modifications.

- There was a question on whether there are exemptions in the bill for journalists. We explained that there is a general carve-out in the bill for legitimate purposes of journalism.
- There was a discussion on the purpose of Section 11 of the bill. There is an Access to Information Act in force in Malawi. This Act gives individuals the right to request information from certain entities. When somebody is requesting information and that includes personal data of third parties. The intention was to give MACRA the opportunity to coordinate with the Human Rights Commission so that there are no conflicts in implementing these two laws that potentially could overlap.

Day 2

On the second day of stakeholder consultations, Jason Blechman presented Guidelines on Data Breach Notifications and Lale Tuzmen presented Rules on Complaints and Investigations.

There was a discussion of whether the law introduces a requirement to retain data for a certain period. We explained that there may be requirements under sector-specific laws and this act does not supersede those requirements. The bill provides that data that is no longer needed should be deleted.

There was also a discussion of how a deceased person's family can access the data. This led to a more nuanced discussion around what is considered permissible processing and what is not.

We received feedback on the complaint timeline under the Draft Data Protection (Registration and Fees) Rules, 2022. Specifically, a stakeholder underlined that after the preliminary review of complaints, the Authority's requirement to promptly notify the complainant of its determination was unclear. We incorporated it into the 10-business day timeline applicable to the Authority's determination on whether it admits or rejects a complaint.

There was a discussion of whether the law applies to the Authority and whether the complaint and investigation mechanisms can be used against MACRA for its processing of personal data if it receives such data, for example from telecommunications operators or other organizations it may be regulating or investigating. We explained that there is nothing that exempts the Authority as a data processor or data controller.

Written feedback received from stakeholders

We have received feedback from MCM on the Draft Data Protection (Registration and Fees) Rules, 2022:

- MCM noted that with respect to the annual fees in Rule 6, it should be clarified whether fees are paid in arrears (i.e., paid at the end of the annual registration period in respect of the registration period that has ended) or in advance (i.e., paid at the end of the annual registration period in respect of the upcoming registration period). We have amended paragraph (1) to clarify that the payment will be made in advance.
- MCM further noted that submitting a fully updated registration prior to the third, sixth, ninth (etc.) anniversary of initial registration submission would be burdensome for a data controller or data processor of major importance because the registrants are subject to the obligation to notify the Authority of any changes to the information they submitted to the Authority when registering. However, the obligation to notify the Authority of changes applies only to significant changes. There is a risk that organizations neglect to keep the Authority informed, and a regular

submission serves to keep them current. We amended Schedule 2 to include all details in the registration submission and an additional column in which the registrant can indicate the information they are changing.

- It was also recommended that instead of reductions and increases to fees (resulting from a change to the number of individuals whose data it processes) taking effect on a registrant's next due date, they take immediate effect on a pro rata basis during the year. We have not implemented this recommendation because this would create burdensome complexity monitoring requirements, including when the number of individuals fluctuates above and below a tier level. MCM was concerned that if fees decrease significantly (e.g., from K500,000 to K50,000) during a registration period due to a reduction in annual revenue, then it is arguably unfair and economically burdensome for the registrant nevertheless to pay K500,000 at the end of that registration period. Opening the door to a pro rata refund in such a scenario would be disproportionately burdensome for the Authority compared to the financial burden that data processors or controllers could theoretically carry. In addition, we believe the annual cut-off is fair because the fees could increase from K50,000 to K500,000 within a registration period and the registrant would still be paying the lower amount until the next registration period.
- MCM further expressed concerns about the provision stating that a former data controller or data processor of major importance will not be eligible for a refund of any portion of the annual fees paid for the annual registration period in which it was removed from the register. For the same reasons as above, we have not revised the approach. As explained above, a pro rata refund would be bureaucratically burdensome for the Authority compared to the financial burden that data processors or controllers would carry when they are removed from the register early in their registration cycle.
- MCM proposed that the form in Schedule 2 include all the details in the registration submission and an additional column in which the registrant can indicate the information they are changing. We accommodated this suggestion and revised Schedule 2.
- Similarly, we implemented MCM's suggestion that Schedule 3 include information that indicates the name and the address of the registrant and date of initial registration.

We have received feedback from MCM on the Draft Data Protection (Registration and Fees) Rules, 2022:

- MCM suggested amending the definition of "Data Protection Office" to include a reference to the section in the Act that establishes the Data Protection Office. The definition includes "established under section 7 of the Act." Since this was already implemented in the rules, we have not changed the existing definition.
- In terms of complainants lodging complaints in writing through various means, MCM noted that some may not be able to lodge complaints in writing, e.g., persons who are visually impaired or persons who are not able to write. We added a provision that is a person wishing to lodge a complaint is not able to do so in writing, the Authority will provide that person with reasonable assistance in making their complaint.
- MCM proposed that, when informing the data subject of its decision to reject the request for non-disclosure, the Authority should inform the data subject of their right to withdraw their complaint. We implemented this suggestion and added it to Rule 6(3).
- MCM noted that in the complaint form in Schedule 1, it is not clear which of the information required in the form is mandatory and which is voluntary. To clarify, we added the following

instructions to the top of the form: “Please fill in all the boxes below. Where the requested information is not applicable, please insert “n/a” to the corresponding section.”