Case 202300315

Enforcement Order

Ministry of Planning, Agriculture, Housing, Infrastructure, Transport and Development

1 November 2024

SUMMARY

A member of the public submitted a complaint to the Ombudsman under the Data Protection Act (2021 Revision) (DPA) against the Ministry of Planning, Agriculture, Housing Infrastructure, Transport and Development (the "Ministry") and the Department of Planning (the "Department") hereinafter referred to as the data controllers. The complainant alleged that his personal information relating to his employment was disclosed to the public on more than one occasion.

After investigating this complaint, the Ombudsman issued an information order and a subsequent enforcement order, finding that the data controllers contravened the seventh data protection principle and section 16 due to a lack of appropriate organizational measures and failure to provide a breach notification within the statutory timeframe, which is an offence.

The Ombudsman ordered the Ministry and Department to have the data protection policies and procedures finalized and approved by 18 November 2024.

A. BACKGROUND

[1] On 11 August 2022, the complainants' personal information was discussed on Cayman Marl Road's ("CMR") "Cold Hard Truth" broadcast in such detail that the average listener could reasonably identify him and resulted in a number of calls to the complainant.

On the same day the complainant sent the snippets of the above broadcast to the Director of Planning via WhatsApp messenger, informing him of the disclosures and expressing his concerns with some of the host's utterances, and saying that she spoke about information that was mentioned in recent internal communications he received.

The complainant provided us with screenshots evidencing the notifications to the Director of Planning about the disclosures made by CMR.

[2] On 9 May 2023, the complainant's personal details were again discussed on CMR's "Cold Hard Truth" broadcast. From the on-air discussion the complainant alleged that it is implied in the broadcast discussion that the information may have originated from within the Ministry and/or the Department of Planning.

[3] On 12 May 2023, the complainant made a complaint to our office alleging that the data controllers appeared to have disclosed personal information relating to his employment within the Department of Planning to the public, which appears to have occurred on more than one occasion. The complainant stated that six days after he received a notice of transfer to a different role within the Ministry during a meeting with the Chief Officer and HR Manager, the on-air discussions ensued.

[4] We accepted the complaint on 23 May 2023 and opened an investigation under section 43 with the abovenoted case file number.

[5] On 22 February 2024, we contacted the Ministry and the Department regarding the complaint and to obtain some additional information to further assess the matter.

[6] On 6 March 2024, The Ministry's Data Protection Officer acknowledged receipt and advised a response would be provided within 30 days.

[7] On 8 April 2024, we requested an update from the Data Protection Officer.

[8] On 30 April, the Data Protection Officer responded advising that she was still working on the matter and would provide an update soon.

[9] On 1 May 2024, we requested a tentative timeframe in which we could expect to receive the response.

[10] On 2 May 2024, the Data Protection Officer confirmed that a response would be provided within a week.

[11] On 3 June 2024, we contacted the Data Protection Officer requesting a response to the following questions, which were outlined in the original email sent on the 22 February 2024:

> *"1. Whether the Ministry and/or the Department of Planning is aware of the CMR broadcasts in August 2022 and May 2023, in which the complainant's employment information was discussed.*
>
> *2. Whether the Ministry has investigated how such information came to be in the public domain. If so, please provide us with a copy of the investigation report.*
>
> *3. In any of the instances when personal data appears to have been disclosed, did the Ministry and/or the Department of Planning consider whether a personal data breach had occurred, and whether the data subject and the Ombudsman should be notified, as required by law?"*

Additionally we advised that a response was required by close of business on Monday 10 June 2024, otherwise an Information Order would be issued. The Data Protection Officer acknowledged receipt on 3 June 2024.

[12] On 11 June 2024, the Ministry issued a response to our questions as follows:

> *1. The Ministry was not aware of the CMR broadcast of August 2022. However, the Ministry was made aware of CMR's broadcast of May 2023 when the complainant sent an email on 12th May 2023 addressed to the Chief Officer and copied to the Director of Planning, with an mp4 file of the broadcast.*
>
> *As stated in your letter, the Department of Planning was made aware of CMR's broadcast of August 2022 via a WhatsApp message from the complainant to the Director of Planning.*
>
> *2. Once the Ministry became aware of the May 2023 broadcast, an informal investigation was conducted. There was no evidence that the Ministry's staff disclosed the complainant's personal information. No formal investigation report was produced at the time.*
>
> *3. The Ministry's investigation (of the May 2023 complaint) was treated as having received an internal complaint. The complaint was not investigated at the departmental level. As a result of these complaints, and to better facilitate the ability to identify and thoroughly investigate a data protection*

breach, both the Ministry and the Department of Planning has since assigned a member of each team as Data Protection Leaders.

Mitigation Efforts: In addition to the efforts mentioned above, the Ministry and Department of Planning have undertaken to:

1. Ensure all staff are aware of the CIG Privacy Policy which includes personal data breach notification.

2. Ensure all members of staff have either undergone or are undergoing data protection training. Both entities maintain up-to-date training logs.

3. Ensure the relevant policies are in place. Both entities are in the late stages of drafting their Data Protection Policies."

[13] Following our review and assessment of the responses, on 26 June 2024 we sought responses to some additional clarifying questions. We asked when the informal investigation was conducted and if a report was ever produced, and if the Ministry was aware of any other entities outside of the Ministry and Department being aware of the complainant's information. Secondly, we requested the appointment dates of the Data Protection Leaders. Lastly we requested implementation timeframes and details concerning the data protection policies, privacy notices, and frequency of staff training.

[14] We followed up for a response on 16 July 2024. Based on a history of delayed responses, the Ombudsman had to issue an Information Order on 14 August 2024, under section 44 of the DPA to obtain the required information, citing 30 August 2024 as the deadline for the response. The data controllers acknowledged receipt of the Information Order.

[15] On 27 September 2024, the data controller advised the complainant of the personal data breaches which occurred on 11 August 2022 and 9 May 2023. Additionally, the data controller responded to the Information Order and formally filed breach notifications concerning the CMR broadcast discussions on the stipulated dates. The Ministry advised that the following:

> *"1. The informal investigation commenced once the Ministry became aware of the information being in the public domain.*

2. The Ministry is not aware of any other entity who would have been privy to this information.

3. No formal investigation report has been produced.

4. The Data Protection Leader for the Ministry was appointed on July 6th 2023; the Data Protection Leader for the Department of Planning was appointed on October 18th 2023.

5 a. The Ministry's resources were completed in July 2024 and are undergoing internal reviews and edits at the senior management level. This includes the Internal Privacy Notice the Ministry's entities including the DoP.

Emails to staff regarding trainings were sent out initially on 27th October 2023 advising staff to complete CIG's Introduction to Data Protection course through the Civil Service College and in person by the Information Rights Unit. New staff are advised shortly after appointment to also undertake the Introduction to Data Protection Trainings…

b. The DoP confirms that the Data Protection Policy and External Privacy Notice are complete and have been reviewed and approved by The Director of Planning and The Attorney Generals Chambers in June 2024. These new polices have not yet been uploaded to the website of the DoP. The DPL is awaiting a scheduled departmental sensitization on the new policies before going live on the website… It is the DoP's intention to formally introduce all employees to the newly crafted data protection policies along with executing interactive sessions via scenarios/activities of relatable data protection cases.

<u>Mitigation Efforts</u>
In addition to the efforts mentioned above, the Ministry has undertaken to inform the complainant as well as the Ombudsman of the breach as required in accordance to the Data Protection Act, section 16."

[16] Whilst the Ministry and Department responded to the Information Order it is apparent that both entities contravened the Data Protection Act. To further assess the matter, a breach severity assessment was conducted. This did not meet the threshold for a monetary penalty.

B. CONSIDERATION OF ISSUES

a) Whether the data controller had appropriate technical and organisational measures in place before the breach to meet their obligations under the seventh data protection principle.

[17] The seventh data protection principle in the DPA provides:

> *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*

[18] Extensive guidance on this principle, and all other requirements under the DPA, is available on the Ombudsman website.[1]

Assessment of Technical Measures

[19] Based on the information obtained throughout the course of the investigation, an apparent lack of organisational measures was a major contributing factor to the breaches that occurred and it was not apparent that technical measures played a major role. As such they are not considered and addressed in this order.

Assessment of Organizational Measures

[20] The Ministry stated that an informal investigation was conducted under the auspices of an internal complaint when they became aware of the information being in the public domain, although no formal report was ever produced. It is disappointing that the investigation into this matter was seemingly so perfunctory, and it does not appear that any serious efforts were made to investigate the source of the breach. No detailed findings of the investigation were shared with the Ombudsman.

[1] Ombudsman, 'Seventh Data Protection Principle – Security – Integrity and Confidentiality', Guide to Data Protection Law 2017 for Data Controllers, https://ombudsman.ky/data-protection-organisation/data-protection-principles/seventh-data-protection-principle-security-integrity-and-confidentiality

[21] The Data Protection Leader for the Ministry was appointed on July 6th 2023; the Data Protection Leader for the Department of Planning was appointed on October 18th 2023, both appointments occurred following the incidents.

[22] The Ministry stated policy resources were completed in 18 July 2024, however have not been finalized and are undergoing senior level review. The Department policy resources were approved by senior management and the Attorney General's Chambers in June 2024.

[23] Staff training was conducted in April and May 2024, however the efforts were interrupted due to an issue on the training system and the subsequent discontinuation of the course until October 2024. The Department was to hold a department wide mandatory data protection sensitization session on 24 October 2024. An additional session to introduce all staff to the new data protection policies and interactive sessions is envisaged, however no date for this session was provided to our office.

[24] Considering all of the elements outlined above, it is evident that the data controllers were not proactive in their handling of data protection matters prior to these incidents. The lack of internal policies and privacy notices highlights the Ministry and Department's failure to have proper documented guidance to assist in the identification and prevention of personal data breaches and appropriate response handling after they occurred. Additionally such policies and related employee training play an integral role in ensuring that personal data is being processed in a manner that is compliant with the DPA.

[25] If the data controllers had appropriate organisational measure in place they would have been better equipped to respond in a manner compliant with section 16 of the DPA in particular the Department who was made aware of the first occurrence, and could have potentially prevented the second breach.

[26] In conclusion, the data controllers did not meet the requirements of the Seventh Data Protection Principle resulting in the disclosure of personal data on two separate occasions. The Ministry and Department failed to implement appropriate organizational measures which in this matter include the utilisation of proper internal governing documents, data protection leaders' appointments and consistent staff training to address the risk associated with the processing of personal data.

(b) Whether the data controllers complied with section 16 of the DPA when the personal data breach was brought to the Ministry and Department's attention in May 2023.

[27] Section 16 in the DPA provides:

> *(1) In the case of a personal data breach, the data controller shall, without undue delay, but no longer than five days after the data controller should, with the exercise of reasonable diligence, have been aware of that breach, notify the data subject of the data in question and the Ombudsman of that personal data breach, describing –*
>
> *(a) the nature of the breach;*
> *(b) the consequences of the breach;*
> *(c) the measures proposed or taken by the data controller to address the breach; and*
> *(d) the measures recommended by the data controller to the data subject of the personal data in question to mitigate the possible adverse effects of the breach.*
>
> *(2) A data controller who contravenes subsection (1) commits an offence and is liable on conviction to a fine of one hundred thousand dollars.*

[28] Extensive guidance on personal data breaches, and all other requirements under the DPA, is available on the Ombudsman website[2].

[29] During our initial assessment of the matter, on 22 February 2024 we wrote to the Department and Ministry and posed the following question:

- *"In any of the instances when personal data appears to have been disclosed, did the Ministry and/or the Department of Planning consider whether a personal data breach had occurred, and whether the data subject and the Ombudsman should be notified, as required by law?"*

On 10 June 2024 , the Ministry responded and stated:

[2] Ombudsman, Personal data breaches, Guide to Data Protection Act for Data Controllers, https://ombudsman.ky/data-protection-organisation/personal-data-breaches

"The Ministry's investigation (of the May 2023 complaint) was treated as having received an internal complaint. The complaint was not investigated at the departmental level. As a result of these complaints, and to better facilitate the ability to identify and thoroughly investigate a data protection breach, both the Ministry and the Department of Planning has since assigned a member of each team as Data Protection Leaders."

[30] In the Ministry's response dated 10 June 2024, it was further stated that the Ministry was not aware of the disclosure on August 2022 CMR broadcast however was aware of the May 2023 disclosure on CMR which was sent by the complainant to both the Chief Officer for the Ministry and the Director of the Department. After the Ministry became aware of the May 2023 disclosure an informal investigation was undertaken which was treated as an internal complaint and no formal report was produced.

[31] On 27 September 2024 we received a breach notification for the August 2022 and May 2023 breaches from the Ministry. Additionally on the same day the Ministry notified the complainant of the breaches, and outlined the future mitigating factors put in place such as the appointment of Data Protection Leaders for the Ministry and Department, development of policies and privacy notices and the implementation of a robust staff training programme and apologized for the fact that the breaches were not prevented and for the resulting consequences.

[32] **Therefore, I have determined that the data controllers failed to comply with section 16(1) of the DPA.**

C. FINDINGS AND DECISION:

For the above reasons, I make the following findings and decisions:

- Seventh data protection principle:
  The data controller did not meet the requirements of the seventh data protection principle since personal data was not being processed in a manner that ensured its protection against unauthorised or unlawful processing and against accidental loss, destruction or damage by utilising appropriate organisational measures to ensure an appropriate level of security that is commensurate with the level of risk associated with the processing activities undertaken:

I. The lack of organizational policies, such as the absence of Data Protection Leaders, and data protection policies, privacy notices and data handling policy were not in place to govern and facilitate appropriate management of the data controllers' data protection obligations. Furthermore, the lack of training contributed to the failure of identification and reporting of the breach occurrences and the length of time during which it took to address and resolve this matter.

- Section 16 - notification:
  The data controller contravened section 16(1) of the DPA, because notifications were not provided in accordance with the statutory timeframe, although they were made aware of the potential breaches by the complainant, and it was raised by our office during our initial assessment of the matter. A formal notification was only furnished to the complainant and our office in September 2024.

- Under section 45(1) of the DPA, for the reasons explained above, I require the data controller to take the following steps to bring their entities into compliance as soon as practicable:

  I. The Ministry must finalize, approve and publish its appropriate policies, procedures and privacy notices within 10 days of this order. This is to ensure that personal data is safeguarded and to maintain compliance with the provisions of the DPA. We further require the final versions of these governing documents to be provided to our Office.

  II. The Ministry and Department must implement a formal staff data protection training programme to be completed on an annual basis and a training log must be developed and maintained. Due to the nature of these breaches we implore both entities to highlight, during staff training sessions, the importance of the sixth data protection principle and increase awareness that unauthorized disclosure of personal data can be a criminal offence under the DPA.

Under section 47, a person who has received an enforcement order under the DPA may, within 45 days of receipt and upon notice to the Ombudsman, seek judicial review of the order to the Grand Court.

Sharon Roulstone
Ombudsman