

Case 202400591, 202400592 & 202400716

Enforcement Order

Workforce Opportunities & Residency Cayman

4 December 2024

SUMMARY

Workforce Opportunities & Residency Cayman (WORC) submitted two breach notifications to the Office of the Ombudsman (OMB) under the Data Protection Act (2021 Revision) (DPA). WORC is the data controller in this matter as defined by section 2 of the Act. WORC's response to two FOI requests for work permit statistics breached the personal data of some 37,686 individuals. The OMB was notified of the breach, as required under the Data Protection Act (2021 Revision) (DPA).

During the review of this matter, the OMB issued an enforcement order, finding that the data controller contravened the seventh data protection principle due to a lack of appropriate technical and organizational measures.

The OMB ordered WORC to provide its office with their approved data protection policies and procedures within 30 days.

A. BACKGROUND

- [1] According to WORC, statistics were requested through an FOI request and the person who generated the data included a tab which contained personal data. The Information Manager did not check the data in the spreadsheet, and the record was disclosed in full to two individuals on different days.
- [2] The breach was reported to the OMB on 20 September 2024. It was reported to have taken place on 16 September 2024 at 14:26 and discovered on 17 September 2024 at 04:54 and reported by the person who inadvertently received the data. The second breach of the same

data happened on 17 September 2024 at 04:34 and was discovered on the same day at 04:40 by WORC.

- [3] According to the breach notification received by the OMB, only 32 customers were impacted; the categories of personal data were names, occupations, dates of birth and employers. Further, WORC explained that the breach was low risk due to the report being disclosed to “professionals” who informed WORC of the breach. WORC also believed that since the recipients of the data only saw the first page (32 individuals) of the report, that only those individuals needed to be notified of the breach.
- [4] WORC explained that as part of their containment measures, the individual who generated the report was advised never to provide personal data when dealing with these types of requests. They proposed addressing the breach by contacting the affected individuals, informing them of the breach, and advising them that the breach received by the unintended individuals was deleted and not shared any further.
- [5] At the time of reporting the breach, WORC informed us that the affected individuals had not yet been informed of the breach due to the number (32) of persons affected.
- [6] On 20 September 2024, we acknowledged receipt of the breaches and asked for clarifications in the following terms:
- “Please verify whether the second submission (202400592) is legitimate as it appears to be the same matter; however, you indicated that 0 data subjects were affected. In addition, please send us a copy of the breach notification, which will be or was sent to the 32 affected subjects.”*
- [7] On 22 September 2024, WORC provided the following clarification:
- “It is the same matter, but the statistics were sent to two different persons, so I was of the impression that two reports needed to be filed. For the second breach, I listed zero persons affected as the recipient was not aware that he had received personal data and had not opened the email.”[sic]*
- [8] On 24 September 2024, we asked WORC to provide the correct total for the affected data subjects. This is because the total number of affected individuals includes the total number listed in the report that was disclosed, not a single page or the first page that may have been viewed by the recipient, as stated in their notification to my office.

Furthermore, upon reviewing their notification (not yet sent to the affected individuals), we found that it did not meet the requirements of section 16(1) (a) and (c) of the DPA and recommended that this be addressed immediately.

- [9] On 7 October 2024, we contacted WORC for an update.
- [10] On 9 October 2024, we were informed that the total number of affected individuals was **37,686**. In addition, WORC explained that notification to the affected data subjects was being worked on however, it was extremely time-consuming.
- [11] On 10 October 2024, we spoke to WORC by phone, explaining that there are various ways in which WORC may notify the affected individuals.
- [12] On 21 October 2024, we followed up with WORC concerning their notification to the affected individuals.
- [13] On 23 October 2024, WORC informed us that they were experiencing network issues and advised that we would hear from them soon.
- [14] On 1 November 2024, as we had not heard from WORC, we informed them that the matter should be addressed no later than 8 November 2024, and failure to do so would result in the Ombudsman issuing an Information Order pursuant to section 44 of the DPA.
- [15] On 20 November 2024, we informed WORC that, as we had not heard from them, the Ombudsman would be pursuing further enforcement action.
- [16] Subsequently, OMB Case #202400716, an additional personal data breach notification, was submitted to my office on 25 November 2024. WORC submitted that the breach happened on 19 November 2024 at 06:50 and was discovered on the same day at 06:58. According to WORC's notification, the breach resulted from an email containing 6 customers' personal data being inadvertently sent to a Gmail address. WORC advised that an attempt was made to contain the breach by having the unintended party delete the information and recall the email. In addition, technical measures were being explored to mitigate future breaches.
- [17] Notably, WORC could not provide us with the categories of data impacted and notifications to the affected data subjects as their internal investigations continued.
- [18] On 25 November 2024, we requested the following:

“Please provide evidence that steps were taken to contain the breach and mitigate its effects.

You stated that the data subjects were not formally notified of the personal data breach. Please provide the data subjects with a notification in accordance with section 16 of the DPA and provide us with a copy.

Please also provide copies of WORC’s internal DPA policy and procedures and advise whether all staff have had DPA training and when your organization last provided training.”

[19] On 26 November 2024, WORC responded informing us that they were seeking to verify the data that was breached prior to notifying the affected individuals. Additionally, we were informed that WORC has no internal DP policies and procedures, and staff completed an online training approximately two years ago.

[20] On 27 November 2024, after further review of the breach, we found that WORC needed to revise its breach notification details as the initial number of data subjects and the type of personal data impacted were incorrect.

[21] On 28 November 2024, we requested copies of the breach notifications and all the documents that were breached. WORC provided us with the documents on the same day, as well as a few more details concerning the breach.

WORC explained that “the breach resulted from system limitations and human error, as the Department’s database is not set up to automatically burst permanent residency notification letters to customers, in addition to the fact that there appears to be further processing limitations when working remotely.”

[22] Upon completion of our review, we found that 9 data subjects were impacted and not 6 as originally reported to us; thus, we asked WORC to ensure that the 9 data subjects were notified accordingly.

[23] On 29 November 2024, WORC advised that one data subject had been notified.

[24] On 2 December 2024, we requested copies of all notifications sent to the affected data subjects and were advised that they were being processed and would be sent by the end of the day.

[25] On 3 December 2024, WORC posted the notification under the About Us in the News section of their website.

B. CONSIDERATION OF ISSUES

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

[26] 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.

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

Assessment of Technical Measures

[28] Under the seventh data protection principle, a data controller is required to ensure that appropriate technical and organisational controls are implemented throughout its processing activities, utilising best practices and a risk-based approach to identify, evaluate and mitigate threats to the organisation and its data. In these instances (202400591, 202400592), WORC expressed the insurmountable task of manually searching for contact details for 37,686 data subjects to provide the data breach notification. This procedure should be reviewed in order to facilitate a more expeditious response to personal data breaches and to ensure that appropriate safeguards and compliance with this principle are maintained.

[29] In the case of 202400716, we recognise the need for administrative processes to be appropriately streamlined with little to no system limitations. The lack of appropriate systems resulted in personal data breaches, along with the lack of swift action to resolve the incident. We found that, once again, WORC was unable to address a seemingly low-risk breach

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>

efficiently due to various delays in obtaining the relevant data to address the matter. We were informed that the Computer Services Department (CSD) had to be contacted to retrieve the data that was breached; according to WORC, “The Administrator explained that because the information was sent from Enterprise, [the Administrator] is not able to go back in to see the history.”

Based on the information obtained from WORC, an apparent lack of technical measures contributed to the breaches that occurred and led to significant delays in notifying affected data subjects under section 16 of the DPA.

Assessment of Organizational Measures

- [30] WORC’s response to the breaches gave the appearance of a lack of training and understanding of the requirements outlined in the DPA. The investigation into this matter by WORC was seemingly perfunctory, and it does not appear that any serious efforts were made to ensure that the affected individuals were notified earlier in the process.
- [31] Considering all of the elements outlined above, it is evident that the data controller has not been proactive in handling data protection matters. The lack of internal policies highlights WORC’s failure to have proper documented guidance to assist in the identification and prevention of personal data breaches and appropriate response handling after they occur. Additionally, such policies and internal employee training play an integral role in ensuring that personal data is processed in a manner that is compliant with the DPA.
- [32] In conclusion, the data controller did not meet the requirements of the Seventh Data Protection Principle, resulting in the disclosure of personal data on three separate occasions. WORC failed to implement appropriate organizational measures, which in this matter, included the utilisation of proper internal governing processes, the appointment of a competent data protection leader and consistent internal staff training to address the risks associated with the processing of vast amounts of personal data.

C. FINDINGS AND DECISION:

- [33] For the above reasons, I make the following findings and decisions:

Seventh data protection principle:

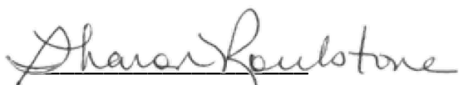
[34] The data controller did not meet the requirements of the seventh data protection principle since personal data was not being processed in a manner that ensured its protection against unauthorised or unlawful processing and against accidental loss, destruction or damage by utilising technical and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

- I. There are no technical measures to assist in handling personal data, as information is sorted manually, and the current in-house system being utilized has deficiencies.
- II. There was a lack of organizational policies, such as the absence of a Data Protection Leader and appropriate data protection policies to govern personal data handling and facilitate requests for information or the internal flow of correspondence.
- III. Furthermore, the lack of training contributed to WORC's inability to identify personal data and report breaches, as well as the length of time it took to address and resolve these matters.

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

- I. WORC must immediately sign-post the notification as an alert on their website's main page.
- II. WORC must finalize, approve, and publish its appropriate policies and procedures within 30 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 within the said 30 days.
- III. WORC must implement a formal staff data protection training programme that is completed annually, and a training log must be developed and maintained. Due to the nature of these breaches, we implore WORC to highlight the importance of the seventh data protection principle and strengthen awareness of the ability to identify personal data and personal data breaches during staff training sessions.

[31] 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