Parliament No:	14
Session No:	2
Volume No:	95
Sitting No:	117
Sitting Date:	22-11-2023
Section Name:	Oral Answers to Questions
Title:	Data Security Incident Involving Personal Data of Members of Shopping Loyalty Programme
MPs Speaking:	The Minister for Communications and Information (Mrs Josephine Teo),Mr Speaker,Ms Hany Soh (Marsiling-Yew Tee),Mrs Josephine Teo,Ms Hany Soh

DATA SECURITY INCIDENT INVOLVING PERSONAL DATA OF MEMBERS OF SHOPPING LOYALTY PROGRAMME

9 Ms Hany Soh asked the Minister for Communications and Information with regard to the data security incident involving the personal data of about 655,000 members of a shopping loyalty programme operated by a luxury resort operator in Singapore (a) whether the incident was reported to the authorities and, if so, when was it reported; and (b) what was the reason provided to the authorities for the three-week delay in notifying affected members.

The Minister for Communications and Information (Mrs Josephine Teo): Mr Speaker, on 7 November 2023, Marina Bay Sands (MBS) announced a breach of its customers' loyalty programme membership data that took place on 19 and 20 October 2023. MBS has since notified affected individuals.

Singapore takes breaches of personal data seriously. The Personal Data Protection Act (PDPA) requires all organisations to put in place reasonable security measures to protect the personal data in their possession or control, to prevent unauthorised access, disclosure or modification. The Guide on Managing and Notifying Data Breaches under the PDPA sets out clear timelines and requirements that organisations must comply with.

MBS discovered the data breach on 20 October 2023, and notified the Personal Data Protection Commission (PDPC) on 24 October 2023. This meets the timeframes for notification to PDPC as set out in the earlier mentioned guide.

The Member may ask why notifications are not required to be made immediately. That is really because in the usual follow-up to the discovery of a data breach, there are usually four things that we would like the organisations to undertake.

First is that they must immediately seek to contain the breach. So, that is the immediate priority. The second is that they must then make best efforts to assess the degree and the extent to which the data breach has resulted in loss of data. The third is then they must assess whether this falls within the requirements for notification, and if it does, then they must proceed to make the report. And the fourth is that they must then evaluate their containment efforts, whether they are secure.

So, there are these four steps, and because the priority is on containment and assessment, PDPC does give the organisation a little bit of time before they make the notification report to the PDPC.

With that as background, let me assure the Member that PDPC is conducting investigations into this incident. It will ascertain whether there was significant harm to affected individuals and correspondingly, whether affected individuals were notified in a timely manner. PDPC will provide their findings in due course.

Mr Speaker: Ms Hany Soh.

Ms Hany Soh (Marsiling-Yew Tee): I thank the Minister for her response to my Parliamentary Question. I have a few supplementary questions in relation to that.

Firstly, in relation to the PDPC's investigation findings, do we have an estimated timeline as to when that will be completed and whether that would be subsequently published to the public for information?

Secondly, subsequent to the reporting by MBS to the PDPC, whether the PDPC has received any reports from members who are affected, especially, and how this particular incident has affected these members and whether any of them has been further assisted since then?

Thirdly, this is in relation to whether the Ministry or the PDPC would consider it necessary to impose further specific or enhancement of obligations to these organisations that possesses large volumes of personal data, for example, through licensing conditions, where applicable?

Mrs Josephine Teo: Mr Speaker, I thank the Member for her supplementary questions. Let me try to address them in turn.

The first is on whether the findings of its investigations will be made public – the answer is yes. As to how long that will take, it goes to the complexity of the investigations. And so, it is difficult to say in advance what the duration is likely to be.

Her second question relates to whether there were any follow-ups from affected members of MBS. The PDPC received reports from two of those members who were affected. Essentially, they wanted to draw the PDPC's attention to this, in case it was not notified, or it was not yet aware of the breach. And the second is that they also asked that the PDPC take MBS to account for this breach which, of course, the PDPC intended to do in any case.

As to how these affected members were being assisted by MBS, I think, in the first place, it is most important for the members to know what types of data have been accessed or revealed as a result of this breach. And so, when MBS notified the affected members, it did clarify that the types of personal data that

were revealed, included the name, contact information, country of residence and membership number as well as tier. This was the extent of the breach that the MBS was able to ascertain.

It further provided advice to the affected members on how they could safeguard their accounts with MBS, as well as other kinds of personal information. As a responsible measure, they provided a contact for follow-up enquiries, in case the affected members wanted to clarify on various other aspects.

Ms Soh's third question had to do with the organisations that could be in possession of large volumes of data. Our position today already states that a higher standard of personal data protection is required when organisations hold large quantities of different types of personal data or hold data that might be more sensitive, such as insurance, medical and financial data.

In such cases, organisations are required to implement enhanced data protection practices as stipulated in the PDPC's guide to data protection practices for information and communications technology (ICT) systems.

In addition, the PDPC has issued an advisory guideline on enforcement for data protection provisions that makes clear that failure to put in place adequate safeguards for large volumes of sensitive personal data can be taken as an aggravating factor in calculating the level of penalties to be imposed on an organisation. I hope that addresses the Member's questions.
