Parliament No:	13
Session No:	2
Volume No:	94
Sitting No:	102
Sitting Date:	1-4-2019
Section Name:	Oral Answers to Questions
Title:	Role of Personal Data Protection Commission in Investigating Blood Donors' Data Leak
MPs Speaking:	Ms Sylvia Lim (Aljunied),Mr Speaker,Ms Sylvia Lim,The Minister for Communications and Information (Mr S Iswaran),Ms Irene Quay Siew Ching,Mr Dennis Tan Lip Fong (Non-Constituency Member),Mr S Iswaran,Ms Irene Quay Siew Ching (Nominated Member),The Senior Minister of State for Health (Mr Edwin Tong Chun Fai),Mr Dennis Tan Lip Fong,Mr Edwin Tong Chun Fai,Miss Cheng Li Hui (Tampines)

ROLE OF PERSONAL DATA PROTECTION COMMISSION IN INVESTIGATING BLOOD DONORS' DATA LEAK

13 Ms Sylvia Lim asked the Minister for Communications and Information regarding the recent data leak of more than 800,000 blood donors' personal information from the database of HSA (a) what is the role of the Personal Data Protection Commission in investigating this incident; and (b) whether any review is being done to ascertain whether HSA has acted reasonably in protecting the personal data including whether the contractual obligations between HSA and its IT vendor reasonably safeguarded the personal information entrusted to these parties.

14 Ms Irene Quay Siew Ching asked the Minister for Communications and Information in view of data breaches across public IT systems (a) whether it is justifiable for public agencies to be exempted from Personal Data Protection Act; (b) what recourse do citizens have, other than to complain to agencies or seek civil action; and (c) whether there should be a tangible penalty meted out to these public agencies for public accountability.

The Minister for Communications and Information (Mr S Iswaran): Mr Speaker, may I have your permission to take Question Nos 13 and 14 together, please?

Mr Speaker: Yes, please.

Mr S Iswaran: Mr Speaker, with regard to the incident involving HSA, the Personal Data Protection Commission (PDPC) is investigating Secur Solutions Group Pte Ltd, which is a private company and

vendor of IT services to HSA. If found to be in breach of the Personal Data Protection Act (PDPA), PDPC will take the appropriate enforcement actions against the company, such as issuing directions and imposing financial penalties.

The Senior Minister of State for Health has earlier outlined the review of HSA's data security policies and practices that is being undertaken. As HSA is a Government agency, the Smart Nation and Digital Government Group is also conducting an investigation into the incident.

Ms Quay has asked if it is justifiable that public agencies are exempted from the PDPA. Implicit in the Member's question is the presumption that public sector agencies are not accountable for their data protection practices or not held to a high standard because the PDPA does not apply to them. That is wrong and simply not the case. Public sector agencies are subject to a different piece of legislation and other regulations. In particular, public sector agencies have to comply with the Government Instruction Manuals and the Public Sector (Governance) Act (PSGA). Collectively, they have comparable if not higher standards of data protection compared to the PDPA, and similar investigations and enforcement actions are taken against data security breaches.

I have previously explained in Parliament why we have adopted this approach. To reiterate, the PDPA does not apply to public agencies because there are fundamental differences in how the public sector operates, which requires a different approach to personal data protection when compared to the private sector. In order to enable a whole-of-Government approach to the delivery of public services, personal data has to be managed as a common resource within the public sector. The considerations are different in the private sector, as there is no such expectation of a holistic approach to the delivery of commercial services across private organisations.

Citizens have the same recourse for a data breach in the public sector as with the PDPA. Where citizens suspect that their data has been mishandled by a private sector organisation, they can lodge a complaint with PDPC; or with GovTech, if a public sector agency is involved. In practice, there are no wrong doors and the complaint will be directed to the relevant agencies for follow-up. Affected individuals can also seek mediation or take civil action against the organisation or agency which mishandled the data.

The Member has asked whether tangible penalties should be imposed on public agencies for public accountability. Public officers who flout the Government's data security rules, and are found to have misused or disclosed data in an unauthorised manner, could be held criminally liable under the PSGA. The penalties include fines of up to $5,000 or a jail term of up to two years, or both. It is not meaningful to impose financial penalties on public sector agencies because the cost of such penalties would ultimately have to be borne by the same public purse.

Mr Speaker, over the years, the Government has progressively enhanced security measures to safeguard sensitive data. The Government has also increased the number and types of internal IT audits, to check on agencies' data access and data protection measures. Nevertheless, recent data-related incidents have underscored the urgency to strengthen data security policies and practices in the public sector.

Therefore, the Prime Minister has convened a Public Sector Data Security Review Committee to conduct a comprehensive review of data security practices across the entire Public Service. This includes measures and processes related to the collection and protection of citizens' personal data by public sector agencies, as well as vendors who handle personal data on behalf of the Government. While individual agencies are investigating and taking action on the specific incidents, this Committee will undertake a comprehensive review across the public sector, and incorporate industry and global best practices to strengthen data security.

This review will help to ensure that all public sector agencies maintain the highest standards of data governance. This is essential to uphold public confidence and deliver a high quality of public service to our citizens through the use of data. The work of this Committee will complement our efforts to achieve our Smart Nation vision. The Public Sector Data Security Review Committee will submit its findings and recommendations to the Prime Minister by 30 November 2019.

Mr Speaker: We will take the supplementary questions for the earlier Parliamentary Questions as well as for these two. Miss Cheng Li Hui

Miss Cheng Li Hui (Tampines): I have two supplementary questions. It was reported that the server was also accessed by several other IP addresses. What do we know about this access? Is it by foreigners or locals and will we be pursuing any actions on them? Do they have the information on the blood donors as well? For those who failed to donate their blood due to illnesses, can this sensitive information be accessed?

The Senior Minister of State for Health (Mr Edwin Tong Chun Fai): On Miss Cheng's latter question, that information was not on the server that was compromised. Only registration related information was on that server. And if I can just cite for Miss Cheng this relevant portion from the vendor's statement. It says that the information that was on that server were NRIC, gender, number of blood donations, dates of the last three blood donations and in some cases, blood type, height and weight.

As for the first point, the unauthorised access is from various locations. That is still being looked into and when we have a fuller position on this and have more clarity, we will provide those answers.

Ms Sylvia Lim (Aljunied): Mr Speaker, I have three supplementary questions for Minister Iswaran. The first is, I am glad to hear that he confirmed that the private sector vendor Secured Solutions Group is actually governed by the PDPA and that PDPC is looking into their conduct. My first question will be, is the PDPC going to wait for the outcome of the HSA investigation and then, follow on from there or is it concurrent?

The second question is, it was mentioned that the Prime Minister has now convened a cross-Government committee chaired by Deputy Prime Minister Teo to look into standards of Government IT security. Does this confirm that the Government is actually not satisfied and that the standards so far have been wanting in the public sector?

Finally, the third question, which is an interesting one, is Minister's answer to Nominated Member Quay's question about financial penalties on organisations. He mentioned that it was not meaningful to fine public agencies because the fine would in the end come from the public purse. But can the central

Government not operate on the premise that no additional money is going to be provided to public agencies to pay fines, and therefore, the agencies would just have to cope with cuts somewhere else to pay these fines, whether it is from bonuses of Senior Management or whatever it is? Because there is still an important signalling effect that the Government is prepared, as an organisation, to abide by the same standards it expects of small businesses.

Mr S Iswaran: Mr Speaker, I thank the Member for her questions. Firstly, on whether the PDPC's investigations would be concurrent, the answer is yes. But clearly, we would have to be informed by what is happening also in some of the other activities because they have some inter-related factors. But the answer is, the investigations will proceed concurrently.

The second question is, what does the establishment of the Public Sector Data Security Review Committee mean. I think the Member is trying to score a political point here and I want to make it categorically clear. The Government has been working, that is why I said so in my answer, consistently working and improving data security standards. There is a list of things that we have been doing over the years and I think this has been explained in the House many times in response to the Member's questions and that of many other Members as well.

The key point here is that, because there has been a series of these incidents in recent times, the Prime Minister and the Government have assessed that we need to take a holistic look again. That does not mean, that what we have is inadequate or lacking, but what it does mean is we should ensure that we put total effort to ensure that we leave no stones unturned in ensuring the highest standards of are met in the public sector when it comes to data security. If there is something that is to be learnt, whether it is from best practices in the private sector or from global companies, that is something we will be very happy to learn from and incorporate in the Government's practices.

Finally, on the point on financial penalties, and the Member makes the point about signalling effect. I would say, that first of all, in fact I think the term "ownself check ownself" was coined by a Member of her party. So, if you fine yourself, you do ask the question, what is the signalling effect there. It is far important that the signalling effect is that, you are taking this issue seriously and holding relevant people accountable. So, that is why, in the way we go about this, the penalties are focused on the individuals, officers, who have made decisions or taken actions which were deemed to be not compliant, and therefore, there are the consequences that I spelled out.

Having said that, I think, when you take action against an organisation in the public sector, the reputational impact on that organisation and leadership is significant. I think the Member will concede that, that in itself is also a major signalling point, because no organisation, public or private, wants to have its reputation tarnished. Having said that, we are prepared to look at all means, to ensure there is clear accountability and ensure that in the public sector we have the highest standards of data security. That is why, this committee has been set up and we will be open to suggestions. If the Member has interesting ideas on this, we would be happy to hear from her.

Ms Irene Quay Siew Ching (Nominated Member): The Minister reassured the House that we have the various acts to impose a high standards of responsibility on public agencies. However, upon reviewing

that, there seems to be a lack of clarity in this Act regarding accountability for data breaches. The focus seems to be on misuse of data. Can Minister clarify?

My second supplementary question is, Minister informed the House that the public agencies have regular mandatory internal audits in place to ensure public agencies comply with these standards for data protection and security of ICT systems. In that case, why are these potential lapses not surfaced during previous internal audit checks?

Mr S Iswaran: May I just seek a clarification from the Member, Speaker?

Mr Speaker: Yes, please.

Mr S Iswaran: When you say the Act does not refer to data breeches, only data misuse, are you referring to the Public Sector (Governance) Act or are you referring to PDPA?

Ms Irene Quay Siew Ching: I am referring to the Public Sector (Governance) Act, Official Secrets Act, Income Tax Act and Infectious Diseases Acts.

Mr S Iswaran: Yes, and have you also looked at the Instructions Manual (IM) 8? Because I think when you look at them holistically, it will be clear, that the issues with data, whether it is a breach or misuse, and when can I argue that there is a kind of continuum here. But let me assure you, when you have a breach of data, you have to establish why it occurred. If it is because of misuse, there will be a certain set of actions. If it is because your systems were not in place, it has to result in a different set of actions to correct the systemic errors. If there were certain people accountable for that systemic error, then they have to be held to account as well. So, I think there is a flow in the way this will proceed, in terms of action against Government organisations.

The second point on regular IT audits, why did they not throw up such issues in the past. I think that is an age-old question. You can have audits, I think it is not just in IT, you have it in financial audits, you have got quality audits, but you still have incidents. This is because it is human beings running the system and from time to time, it can happen. I think what is important is that when they occur, we learn from these incidents and set them right, and be transparent about what we are doing and how we are going about it.

Mr Speaker: Mr Dennis Tan.

Mr Dennis Tan Lip Fong (Non-Constituency Member): A question for Senior Minister of State Edwin Tong. Is the Senior Minister of State able to answer any aspect of my questions?

Mr Edwin Tong Chun Fai: Can the Member elaborate on what other aspects have not been answered?

Mr Dennis Tan Lip Fong: No, on my question. Not sure my question has been answered.

Mr Edwin Tong Chun Fai: Mr Dennis Tan's question relate to the circumstances in which the information is placed on the server. How it is that there was access that was gained to the data and whether there was a breach of any law? Those are all matters that are covered by the investigations that are currently on-going, and to the extent possible, when this has been ascertained, we will provide those information.