In the third week of May 2022, the public's attention was once again roused over an alleged data leak involving the personal information of 22.5 million Malaysians of the age between 18 and 82 years. It was reported that such personal information was allegedly leaked from the database of the National Registration Department ("**NRD**"). The allegation, however, has been denied by the Home Minister, Datuk Seri Hamzah Zainuddin, who said that the dataset did not belong to the NRD. Local tech forums such as Amanz and Lowyat.Net reported that the 160 GB size of database is put on sale on the dark web for US$10,000.

Disappointed but not surprised – is probably the accurate public response towards the breach, considering that this is the second time that an alleged breach at the NRD has been reported when the same thing happened back in September last year involving the sale of personal details of 4 million Malaysians, stolen from NRD and the Inland Revenue Board.

Impact of Personal Data Breach

This massive personal data breach has put the security and interests of the citizens at stake, where it is evident through the rising number of scammers on a daily basis. Personal data such as names, phone numbers, addresses and bank account details have made it easier for scammers to convince people that they are officers from banks, courts or police. Although the cyber scam was yesterday's news, many people are still falling for it as the scammers' tricks keep developing and becoming more unsuspecting in duping the victims due to the scammers having access to the victims' personal data through these breaches. It is an even scarier fact that the personal data are on the dark web's market which is the playground for hackers to facilitate criminal activities and purchase of illegal products and services such as money laundering, drugs, human trafficking, identity theft, pornography, counterfeit money, fake passports and other illegal activities involving personal data.

Not only that, breach of personal data can also jeopardize the national security. For example, in 2016, Russian operatives had purchased stolen information about private citizens of the US, which were then used to open the US bank and PayPal accounts, buy access on the US-based servers, purchase Facebook ads for political rallies and pose as Americans on social media accounts to interfere with the US political system, including the 2016 presidential election.

Malaysia's Position

In 2013, Malaysia enforced the Malaysian Personal Data Protection Act 2010 ("**PDPA**") which spells out the 7 data protection principles to regulate and safeguard the processing of personal data. Breach of any of the said principles by any data user shall amount to a criminal offense under the PDPA and is punishable by a fine of up to RM 300,000 and/or up to 2 years imprisonment. Nevertheless, the PDPA is only applicable to commercial transactions and pursuant to Section 3(1) of the PDPA, the Federal and State Governments are not subjected to the PDPA. Hence, it can be said that people have no recourse against the government for the breach under the PDPA.

Data Breach Involving Government Agencies in Other Jurisdictions and How They Rectify It

There are a number of reported instances where governments in other countries have admitted the vulnerabilities in their system which has caused the leak of their citizens' personal data. To name a few, in September 2021, there was a cyber-attack on the France government's 'France-Visas' website where the personal details of individuals looking to visit or emigrate to the country had been breached. According to the French government ministries, they have immediately implemented measures to secure their visa website to prevent further attacks. The affected individuals have also been notified of the data breach and been given recommendations to protect their personal data and online identities.

In February 2020, the government of Quebec, Canada admitted to a data breach potentially impacting around 360,000 teachers employed in the Canadian province. It was reported that the impacted individuals are given the choice to apply for free credit monitoring and would be notified by the provincial government if their information was disclosed. A dedicated breach hotline has also been set up to sort out the burst.

What Can Be Done?

Despite the limited scope of the PDPA and its non-applicability to the government, there are certain measures that can be taken through legislative reforms to mitigate the risks of the data breach. With regard to the government's accountability, merely amending the PDPA to include a certain degree of liability on the government agencies in safeguarding the

personal data will not do the trick. In order to have a better protection of the personal data, the lawmakers may need to consider adopting the measures taken by other countries which have been proactive in handling cases of personal data breach by their governments, or better yet, enforcing a whole new specific legislation, policy or guidelines which binds the government on its commitment to protect the personal data of the citizens.

In Canada, apart from the Personal Information Protection and Electronic Documents Act (PIPEDA) which covers the handling of personal information by private sectors, there is also the Privacy Act ("**the Act**") which is applicable to federal government institutions that collect, process, use, retain and disclose the personal information of a person. The Act has a schedule listing all the federal government institutions which would be subject to the Act including departments, ministries, agencies, as well as government-linked corporations and their wholly-owned subsidiaries. The Act also clearly spells out how the government institutions may handle personal information, from the collection, use, accuracy, retention and disclosure. Not only that, the Act also provide for complaints from data subject and investigations procedures which shall be handled by the Privacy Commissioner.

Apart from that, the approach taken under the European Union's General Data Protection Regulation ("**GDPR**") in relation to the public sector can also be adopted. One of the requirements under the GDPR with regard to the government agencies that process personal data is to appoint a Data Protection Officer ("**DPO**") who will be responsible, among others, to monitor the compliance of the government agency with the GDPR and other data protection provisions and policies. Furthermore, the GDPR also require the public sector bodies to adhere with specific transparency obligations by providing the data subjects with information such as the identity, contact details and the representatives of the government agencies who are the controller of the personal data, the contact details of the DPO and the purposes of the processing of the personal data as well as the legal basis for the processing.

In addition to that, regular training and awareness programmes should also be conducted among the public officials on data protection and cyber security protocols. By now, the officials should have known that the use of weak password such as '12345' will no doubt give hackers an easy way to break into the government database system and lead to leak of personal data. Not only that, data subjects should also be given their individual right to be compensated from the data users which should include the government agencies for the loses suffered due to the data breach. Last but not least, the government agencies should improve the quality of their database security by investing on an improved cloud-based software, hiring qualified IT officials and improving their IT ticketing strategy to prevent any potential cyber-attacks to go unnoticed.

Conclusion

Despite being ranked among the top ten countries with high commitment to cybersecurity in the Global Cybersecurity Index 2020, Malaysia still has a lot to improve in the area of

privacy and personal data protection. The worrying increase in the number of personal data breaches may require urgent amendment to the PDPA or a new legislation, policy or guidelines for better protection of the citizens' personal data. A robust and transparent investigation must also be conducted to ensure data breach cases are effectively handled with a just outcome.

Written by:

Nur Amalina Azami
Associate
nuramalina@azmilaw.com

Hanizah Mohd Huzin
Senior Associate 1
hanizah@azmilaw.com

Corporate Communications
Azmi & Associates
22 June 2022