Data breach is a big concern, say experts

By QISHIN TARIQ
lifestyletech@thestar.com.my

PETALING JAYA: As the government moves to make the use of the MySejahtera app compulsory, experts are concerned that a data breach could leak sensitive information, increasing the number of scams targeting the public.

However, the Department of Personal Data Protection (JPDP) assured that although the government was not subject to the Personal Data Protection Act (PDPA) 2010, action could still be taken against those responsible for a data leak.

A JPDP spokesperson said the public could file a complaint to the Chief Government Security Office, a unit under the Prime Minister's Department that is responsible for the security of all government assets, or the National Cyber Security Agency.

Errant officers who mishandled the data could be charged under the Official Secrets Act 1972 and the Public Officers (Conduct and Discipline) Regulations 1993, he added.

He had checked with the Crisis Preparedness and Response Centre and confirmed that the data is owned by the Health Ministry and is protected by Section 3 of the PDPA. Section 3 states that the Act shall not apply to the Federal Government and state governments.

Bar Council Information Technology and Cyber Laws Committee deputy chairman Foong Cheng Leong also called for more transparency and accountability if there was misuse of the data.

Details that matter: Members of the public registering themselves the modern or old-fashioned way before entering Petaling Street in Kuala Lumpur.

He said there also needed to be an assurance that data would be destroyed at some point in time, adding, "The law should have all the safeguards that we need."

Universiti Sains Islam Malaysia (Usim) Cyber Security and System Research Unit coordinator Dr Madihah Mohd Saudi said the PDPA had a provision that gave users the right to request for their data to be deleted.

She suggested that the government adopt a feature that allowed users to manually delete their history of check-ins after an appropriate amount of time had lapsed and the data was no longer needed.

She said that although the MySejahtera app, like any other system, was not immune to being hacked, it was still more secure than writing one's name down in a physical logbook, as the info could be easily exploited.

Madihah said that as the app was continuously being updated, it showed that the government was taking steps to improve the system and could even be addressing vulnerabilities if any were discovered.

Cybersecurity specialist Fong Choong Fook questioned what the government had done to protect the data and what process would be used to destroy the gathered information after a certain period of time.

To ensure the successful mandatory adoption of the app, Fong said the government needed to be transparent on its processes and the security controls that were in place.

He predicted there would be an "explosion of scam calls" should the MySejahtera data be leaked, as it kept track of critical information, including a user's movements.

He said this information might not seem sensitive to a layman, but a scammer could use the data to form a profile of a victim.

"They would know I've been to a shopping centre in the morning, then a restaurant next door. With this, a scammer can pretend to be a government official and create a scare story to trick the victim into doing something they otherwise wouldn't," he said.

Fong said the government would need to be more transparent with the data management. If it wasn't, the adoption of MySejahtera could suffer due to a sceptical public, he added.