Your data or your life: Can we have both?

With no foreseeable end in sight yet for the Covid-19 pandemic, some Malaysians are growing concerned about the long-term accumulation of their personal data for contact tracing.

Stories by DINA MURAD
dina@thestar.com.my

EFFECTIVE contact tracing is necessary if we are to combat Covid-19. And for that to happen, Malaysians will have to be willing to share some of their personal data with the authorities – their names, contact details and the places they visit.

It, however, also underscores how important it is for those collecting the data to ensure that the information they use is secure and safe from misuse.

For this to happen, three basic principles must be observed, data protection law expert Prof Abu Bakar Munir explains: transparency, limited data retention and accountability of authorities.

Abu Bakar recognises that in emergency situations like the present Covid-19 outbreak, it is necessary for the Government to collect data for contact tracing and public health purposes.

"However, the Government must be transparent about the purpose of data collection, transparent about the choice of design and be transparent about the benefits of the data collection," he says.

"The success of contact tracing depends on the uptake by the public, and the uptake will depend on trust. And trust will depend on transparency and accountability," he adds.

MySejahtera, the national Covic-19 contact tracing app with approximately 15 million users as of August, is owned and operated by the Government.

It was developed to support the implementation of the Prevention and Control of Infectious Diseases Act 1988 [Act 342] and is administered by the Health Ministry with assistance from the National Security Council (NSC) and the Malaysian Administrative Modernisation and Management Planning Unit (Mampu).

On MySejahtera's Frequently Asked Questions (FAQ) section on its website, the Government assures the public that their personal information "will only be used for the purpose of managing and mitigating the Covid-19 outbreak" and that it will not be shared with any other party.

The app was developed through a strategic cooperation between the NSC, the Health Ministry, Mampu, the Malaysian Communications and Multimedia Commission (MCMC) and Science, Technology and Innovation Ministry (Mosti).

By October, nationwide registration of MySejahtera reached more than 60% of the country's population. This is welcome news because 60% is the threshold for an effective contact tracing ecosystem according to a recent Oxford University study.

Amend the PDPA

But to further improve our current contact tracing system, it is necessary to show accountability and one way to do this is to have the Personal Data Protection Act (PDPA) 2010 also be applied to the Government and not just private entities, says Abu Bakar.

The PDPA regulates the processing of personal data in commercial transactions and protects personal data from being misused. The general principle behind the Act is that any processing of your personal data requires your consent. The penalty for non-compliance is a fine of between RM100,000 to 500,000 and/or between 1 to 3 years' jail.

In the case of Covid-19, the PDPA has provisions which allow for the collection of necessary data in situations which require the protection of "vital interests" relating to the life, death or security of the data subject.

A contentious aspect of the PDPA is that Section 3(1) states that the Act does not apply to the federal and state governments.

"I have been arguing [against the exemption] since the Act was enacted in 2010. It is not in line with international standards to give exemptions under the PDPA to the public sector and Government. It is high time for us to amend the PDPA," says Abu Bakar, who was one of the advisors during the drafting of the law.

Abu Bakar also emphasises the importance of efficient enforcement.

"The Department of Personal Data Protection (JPDP) has issued guidelines for businesses on how to manage the data that they have collected, but we do not know how well these individuals comply with the guidelines. Who are those taking charge, who are those collecting the data, what are they going to do with it and how long will they keep it?," he asks.

There is concern that while businesses may not have any intention to misuse data, the way the data is stored may still not be secure. For example in September, a group of people posed as Health Ministry personnel and stole Covid-19 record books from businesses premises around Melaka.

JPDP's advisory was issued on May 30 as a reference for business entities. It listed out Standard Operating Procedures (SOPs) for contact tracing data collection, processing and storage.

Among the directives imposed by JDPD is that businesses were only allowed to record names, contact numbers, and date and time of visit. While temperature checks are necessary to enter a premise, body temperature does not have to be recorded or noted down as it is sensitive personal data and its recording requires express consent from the data subject.

Personal data collected at business premises to facilitate contact tracing during the Covid-19 pandemic should be deleted or destroyed six months after the end of the movement control order (MCO).

However, due to the continuous extension of the MCO, JPDP will be issuing another advisory which will provide further clarifications on how to dispose collected personal data as it is currently seeking input from MOH and NSC on the allowable retention period for contact tracing data.

Cross-agency effort to step up data protection

JPDP reassures the public that it has been working closely with other law enforcement agencies and technical entities to guarantee the personal data ecosystem would thrive in Malaysia.

"The Covid-19 outbreak has opened up new ways on how we approach problems and tasks in hand. JPDP is always keeping abreast and being well equipped with new methodologies and technologies to combat any issues related to privacy," the department said in response to queries by *Sunday Star*.

It adds that the Health Ministry has reiterated many times through different platforms such as daily briefings and social media that the collected personal data would only be used for contact tracing while businesses entities were given constant reminders never to abuse the personal data collected for purposes other than contact tracing.

In terms of enforcement, the department has conducted 804 inspections in total as of Oct 2 on business premises throughout Malaysia (except Sabah and

Essential app: By October, nationwide registration of MySejahtera reached more than 60% of the country's population, which is the threshold for an effective contact tracing ecosystem according to a recent Oxford University study.

Sarawak) to ensure full compliance on the issued advisory.

"JPDP enforcement teams have also conducted investigations on formal complaints received from the general public whenever their personal data were being used for other purposes such as direct marketing, spam etc. by the Data Users," it adds.

A meeting was conducted on June 19 between JPDP, the Health Ministry, NSC, National Cyber Security Agency (Nacsa), Selangor State Government and Kuala Lumpur City Hall (DBKL) to gather feedback on their contact tracing initiatives. During the meeting, a Personal Data Protection Commissioner urged the parties to adopt the 7 Data Protection Principles and embedded them in their contact tracing applications.

"Although Section 3 of the Personal Data Protection Act 2010 [Act 709] states on the non-application of Act 709 to the Federal and State Governments, by adopting these Principles, this would send a firm message to the general public on the Government's commitment to safeguard the collected personal data and only for the purpose of contact tracing," it says.

Address issues of transparency

Because the data collected goes straight into the app, there is a low risk for businesses to misuse the information. However, lawyer Adlin Abdul Majid, who specialises in data protection, believes that there are still issues that need to be addressed such as introducing more transparency in how the Government uses the information collected by MySejahtera.

"Apps like MySejahtera are OK as long as the Government doesn't misuse it. The issue with the PDPA is that the government is exempt from that law. What we need is to introduce amendments to make the PDPA also apply to federal and state governments," she says.

"When it comes to public health concerns and data protection, it is not a case where one wins over the other. Both are necessary but the key is that we need to have laws in place to regulate the use of data.

"It is not wrong for the Government to collect information [for contact tracing], but there should be protection mechanisms in place," she explains.

Adlin adds that one of the amendments being looked into is the application of PDPA on the Government.

In August, the Government said that it is currently in consultation with relevant agencies to see if there is a need to amend the PDPA. This was in response to a Parliament question fielded by former Communications and Multimedia Minister Gobind Singh Deo on whether measures taken to ensure personal data collected through Covid-19 contact tracing applications was secure.

The benefit for having apps like MySejahtera is that it cuts off businesses from obtaining important personal details such as your name and phone number.

Some unscrupulous parties can sell this information to marketers who then contact members of the public to sell products. In more sinister circumstances, scammers purchase and use contact numbers to dupe and steal from unsuspecting victims.

"It is considered to be misuse if businesses sell our information to third parties without our consent. As far as businesses are concerned, they already have to comply with the PDPA. The area of improvement now is to include the Government under the law," says Adlin.

Meanwhile, JPDP assured the public in August that although the government was not subject to the PDPA, action could still be taken against those responsible for a data leak.

The concern is valid as there has been a precedence of a Government data leak.

Last year, technology news portal Lowyat.net highlighted a flaw in the Petrol Subsidy Programme microsite which could potentially have exposed the details of 2.9 million people identified as belonging to the B40 group that qualify for fuel subsidies. After the alert, the security breach was fixed a few hours later by the Domestic Trade and Consumer Affairs Ministry.

A 2019 study on privacy and surveillance of 47 countries by British tech website Comparitech found Malaysia to be the fifth-worst country in terms of protecting the personal data of its citizens. Malaysia was placed in the "some safeguards but weakened protection" category with a score of 2.64 out of five points. The worst-performing country was China (1) followed by Russia (2), while the best performing countries were Ireland(1) and Norway (2).

Sunday Star has reached out to The National Cyber Security Agency for comment.