



Wednesday, 9 September 2020

Data Privacy Insights: Navigating Contact Tracing during COVID-19 in Asia

Kieran Donovan, Hong Kong
Gen Huong Tan, Singapore

Agenda / Introduction

1. Overview of contact tracing technologies in Asia
2. Singapore
3. Hong Kong
4. Other APAC countries



LATHAM & WATKINS LLP

Overview of contact tracing technologies in Asia

What is contact tracing?

“Contact tracing involves identifying people who have an infectious disease, such as COVID-19, and then quickly identifying everyone who they may have come in contact with to prevent further spread of the disease through isolation and voluntary self-quarantine.”

- Centers for Disease Control and Prevention

- Manual
- Automated

Overview of contact tracing technologies in Asia

- **Australia:** COVIDSafe
- **Hong Kong:** Stay Home Safe
- **India:** Aarogya Setu
- **Indonesia:** Peduli Lindungi
- **Japan:** COCOA (Contact-Confirming Application)
- **Malaysia:** MySejahtera
- **Singapore:** SafeEntry, TraceTogether
- **Thailand:** Mor Chana, Thai Chana
- **Vietnam:** Bluezone

Collection of personal data in light of COVID-19

- To recap - **personal data** is any information which are related to an identified or identifiable natural person.
- Generally, consent, or another legal basis, is required for the collection of personal data belonging to an individual.
- Depending on the jurisdictions, exemptions do exist for public health reasons.



Data Protection Principles

Some common principles to abide by when collecting personal data:

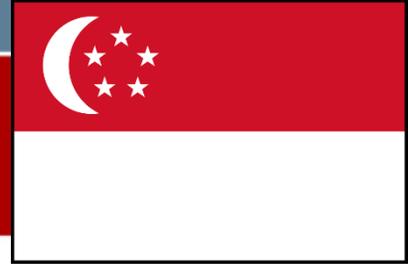
- **Transparency**
 - Be clear in describing the data that is being collected, and the purpose for which it is being collected.
 - Information should only be used for the stated purpose.
- **Data Minimization**
 - Personal data should only be collected where necessary to achieve the stated purpose.
 - Minimize the amount of personal data collected as much as possible.
- **Retention**
 - Data should only be retained as long as is necessary to fulfil the purpose for which it was collected, and destroyed when that purpose is complete.
- **Security**
 - Adopt technical and any other necessary measures to ensure the security of the collected personal data and prevent the personal data from being divulged, damaged, or lost.



LATHAM & WATKINS^{LLP}

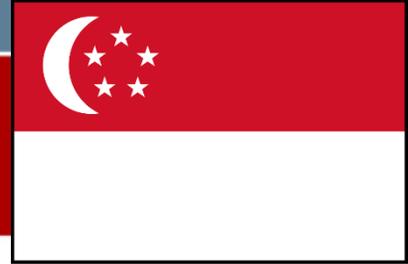
Singapore

Collecting COVID-19 Data



Can you collect health data for the purpose of COVID-19 response measures?	Yes, this is necessary to respond to an emergency that threatens the life, health or safety of other individuals, or for managing the employment relationship.
What types of data can you collect?	COVID-19-related conditions, MCs, test results, NRICs.
Can you collect social media data?	Possible, through exception for publicly available data. But check data minimization.
What do you need to provide before you collect the data?	Notify persons that the collection, use or disclosure of personal data is for purposes of contact tracing and other COVID-19 response measures.
Can you share the data?	If requested by government authorities for contact-tracing purposes, then yes. But otherwise no – unless you have the consent of the person or an exemption applies.
How must you protect the data?	You must make reasonable security arrangements to protect the personal data in their possession from unauthorised access or disclosure.
What if an employee has COVID-19?	The authorities may disclose personal data to an organisation to assist in its contact tracing efforts, or require it to provide personal data of employees for contact tracing purposes.
How long can you retain the data?	You must destroy the data once the purpose for which it was collected is fulfilled. As a benchmark, government applications currently retain information for 25 days.

Contact Tracing & Reporting



Is there a contact tracing application or program available?	Yes. SafeEntry and TraceTogether applications.
Is use of a contact tracing application mandatory?	SafeEntry is mandatory. TraceTogether is not mandatory but employers have been advised by MOM to encourage employees to use the application.
What data must be reported to the relevant authority/government department?	SafeEntry – sends information to government database directly. TraceTogether – if contacted by MOH, user must upload Bluetooth proximity data. In the event of government inspections of workplaces, an employer must show: <ul style="list-style-type: none">• A list of all employees which indicates their work arrangements, shift hours (if applicable), and team number.• Records of COVID-19-related conditions, MCs and test results reported by employees.



LATHAM & WATKINS^{LLP}

Hong Kong

Collecting COVID-19 Data



Can you collect health data for the purpose of COVID-19 response measures?	Yes. It is considered a “reasonable measure” for managing the workplace.
What types of data can you collect?	Reasonable health data (e.g., temperature check, symptoms declaration, travel declaration).
Can you collect social media data?	No. However, the Center for Health Protection may collect personal data from social media to track or monitor potential COVID-19 carriers or patients.
What do you need to provide before you collect the data?	Notify persons that the collection, use or disclosure of personal data is for purposes of being in compliance with the law, e.g. for purposes of contact tracing and other necessary response measures to contain the outbreak of COVID-19. The existing privacy notice may cover such data (although unlikely).
Can you share the data?	No – unless you have the consent of the person or you rely on an exemption (e.g., public health interest).
How must you protect the data?	You must protect the data from unauthorized or accidental access (DPP4).
What if an employee has COVID-19?	You should notify other employees and stakeholders <u>without disclosing the personal data of the infected person.</u>
How long can you retain the data?	You must permanently destroy the data once the purpose for which it was collected is fulfilled.

Contact Tracing & Reporting



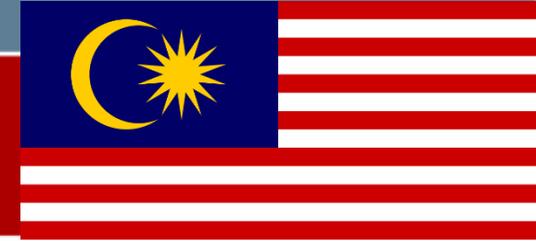
Is there a contact tracing application or program available?	<p>Yes. There is a quarantine monitoring application - mandatory wristbands have been introduced for those arriving from overseas and are required to be worn for a 14 day home quarantine period. The wristband is linked to an app, StayHomeSafe.</p> <p>There is no contact tracing app available otherwise.</p>
Is use of a contact tracing application mandatory?	<p>Yes.</p>
What data must be reported to the relevant authority/government department?	<p>Medical practitioners are required under law to notify the Department of Health of all suspected or confirmed cases of COVID-19. This includes the suspected/confirmed person's identity, health, and location data.</p>
Are there any other noteworthy restrictions or conditions?	<p>Using personal data available on social media to track potential COVID-19 carriers or disclosing their personal information to third parties (e.g., health authorities) is permissible under the PDPO.</p>



LATHAM & WATKINS^{LLP}

Examples from other APAC countries

Collecting COVID-19 Data



Can you collect health data for the purpose of COVID-19 response measures?	Yes.
What types of data can you collect?	Businesses shall only collect minimal personal data of customers or visitors (i.e: name, contact number). This data may be collected either manually or digitally. For both manual and digital data collection, businesses must ensure that the personal data is only collected for the purposes of contact tracing, and that the personal data collected is accurate and not misleading.
Can you collect social media data?	No.
What do you need to provide before you collect the data?	Businesses must display a notice conspicuously to inform persons of the purposes for the collection of their personal data. A specific document must also be used for recording data throughout the CMCO* period.
Can you share the data?	No – unless you have the consent of the person or you rely on an exemption (e.g., public health interest).
How must you protect the data?	Information must be recorded by staff to avoid unauthorized/accidental disclosure of personal information.
What if an employee has COVID-19?	<p>If an employee is infected, employer may notify other individuals who have come into contact with the employee and disclose the identity of the infected employee even if explicit consent has not been obtained, in order to protect the vital interests of the infected employee and other employees.</p> <p>Employers may also disclose the infected employee’s personal data to the health authorities without the employee’s consent to comply with legal obligations and to protect the vital interests of the employee / others where consent cannot be given or reasonably obtained.</p>
How long can you retain the data?	Personal data collected shall only be kept for a maximum of 6 months after the CMCO ends, after which such personal data shall be destroyed or permanently deleted.

Contact Tracing & Reporting



Is there a contact tracing application or program available?	Yes – MySejahtera.
Is use of a contact tracing application mandatory?	Yes - Business outlets must use the government's MySejahtera application as its contact tracing method for their patrons and customers
What data must be reported to the relevant authority/government department?	Contact number, email address, full name, identity card (IC) number, age, gender, ethnicity, and home address - MySejahtera requires these personal details from users who download the app. MySejahtera does not record people's temperatures upon checking in at a location. Extraction of data from MySejahtera only happens when there is a positive Covid-19 case to perform contact tracing activities.
Are there any other noteworthy restrictions or conditions?	The right of data subjects to be given access to his/her personal data held by businesses and to correct such personal data has been suspended during this period

Collecting COVID-19 Data



Can you collect health data for the purpose of COVID-19 response measures?	Yes.
What types of data can you collect?	Organizations should collect as little information as is reasonably necessary for preventing or managing COVID-19. For example: <ul style="list-style-type: none">• whether the individual or a close contact has been exposed to a known case of COVID-19• whether the individual has recently travelled overseas and to which countries.
Can you collect social media data?	No but organisations can collect information about an individual from a third party where it is unreasonable or impracticable to collect that information directly from the relevant individual
What do you need to provide before you collect the data?	Obtain the individual's consent (express or implied) to its collection, and the information is reasonably necessary, or directly related to, one or more of its functions or activities, such as to prevent or manage COVID-19 in the workplace.
Can you share the data?	No – unless you have the consent of the person or you rely on an exemption (e.g., threat to public health).
How must you protect the data?	Take reasonable steps to ensure the security of personal information, including by destroying or de-identifying the COVID-19 related information when it is no longer needed;
What if an employee has COVID-19?	You may also inform other employees that there has been an infected employee and relevant information where necessary to manage the serious health threat.
How long can you retain the data?	You must permanently destroy the data once the purpose for which it was collected is fulfilled.

Contact Tracing & Reporting



Is there a contact tracing application or program available?	Yes - COVIDSafe App
Is use of a contact tracing application mandatory?	No.
What data must be reported to the relevant authority/government department?	Name (or pseudonym), age range, postcode and phone number. Bluetooth data is also uploaded to the server upon testing positive in order for the government to figure out, using signal strength, which contacts need to be notified.
Are there any other noteworthy restrictions or conditions?	The data in the COVIDSafe App cannot be used by private organisations. The data is hosted by AWS in Australia.

Collecting COVID-19 Data



Can you collect health data for the purpose of COVID-19 response measures?	Yes.
What types of data can you collect?	“Necessary” data. This includes name, address, mobile number, travel history, temperature.
Can you collect social media data?	No.
What do you need to provide before you collect the data?	Notify persons that the collection, use or disclosure of personal data is for purposes of being in compliance with the law, e.g. for purposes of contact tracing and other necessary response measures to contain the outbreak of COVID-19. The existing privacy notice may cover such data (although unlikely).
Can you share the data?	No – unless you have the consent of the person or you rely on an exemption (e.g., public health interest).
How must you protect the data?	Personal and sensitive information of an employee should always be protected, and the names of the affected or suspect employees should be scrubbed and deleted while being processed internally as a part of the action plans. Employers should not disclose name of infected person to other employees.
What if an employee has COVID-19?	No legal obligation to report to Government agencies of an infected employee’s COVID-19 status. Employer may inform other employees that there has been an infected employee.
How long can you retain the data?	Protocol states that anonymous data can be shared with any government ministry for the purpose of tackling Covid-19. Any data received should be permanently deleted after 180 days (but no way to ensure this).

Contact Tracing & Reporting



Is there a contact tracing application or program available?	<p>Yes – Aarogya Setu. Mobile app developed by the National Informatics Centre under the Ministry of Electronics and Information Technology.</p> <p>Collects demographic, contact, self-assessment and location data, collectively known as response data. This can be shared by the app’s developer – National Informatics Centre – with government authorities and any third parties if necessary.</p> <p>Location data for the last 30 days will be pinged to the server.</p>
Is use of a contact tracing application mandatory?	<p>Mandatory for all central government employees and private sector employees.</p>
What data must be reported to the relevant authority/government department?	<p>Personal information of suspected and confirmed cases are published publicly: In newspapers and social media to ensure effective containment of coronavirus transmission, including individual’s name, address, mobile number, start date of quarantine, and the police station under which jurisdiction the residents comes.</p> <p>On posters, including suspected cases’ names, quarantine period, and the number of people in the family who have been asked to remain in isolation</p> <p>On certain government websites, including names of suspect and family members, with phone numbers and residential addresses posted on a government website</p>

Collecting COVID-19 Data

Can you collect health data for the purpose of COVID-19 response measures?	Yes.
What types of data can you collect?	An employer may require employees and visitors to provide their temperature readings or to declare if they experience any respiratory symptoms.
Can you collect social media data?	No.
What do you need to provide before you collect the data?	Employers must notify employees that the collection, use or disclosure of personal data is for purposes of being in compliance with the law, e.g. for purposes of contact tracing and other necessary response measures to contain the outbreak of COVID-19.
Can you share the data?	No – unless you have the consent of the person or you rely on an exemption (e.g., public health interest).
How must you protect the data?	Under the PDPA, the personal data shall be collected only to the extent necessary for the relevant lawful purpose, and shall be deleted or destroyed whenever it is irrelevant or no longer needed for the purpose necessary for which it has been collected.
What if an employee has COVID-19?	The CDA requires an employer to notify a communicable disease control officer within three hours of being made aware that a person infected, or suspected of having been infected, with COVID-19.
How long can you retain the data?	To be deleted or destroyed whenever it is irrelevant or no longer needed for the purpose necessary for which it has been collected

**In February 2020, the Minister of Public Health announced that the Coronavirus Disease 2019 or COVID-19 is a dangerous contagious disease under Thailand's Communicable Diseases Act*

Contact Tracing & Reporting

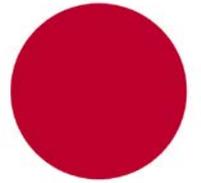
Is there a contact tracing application or program available?	Yes – Mor Chana, Thai Chana, DDC-Care, AOT Airport Application, Sydekick for THAIFIGHT COVID-19
Is use of a contact tracing application mandatory?	Yes. AOT Airport is compulsory for individuals who have travelled or returned from contagious areas outside Thailand and are diagnosed as infected. Sydekick for THAIFIGHT COVID-19 is compulsory for individuals who have been discharged from detention at the quarantine centre and returned to their own domicile for self-quarantine. Mor Chana is voluntary.
What data must be reported to the relevant authority/government department?	Communicable Diseases Act requires an employer, as an owner or a person controlling a business facility, to notify a communicable disease control officer within three hours of being made aware that a person infected, or suspected of having been infected, with COVID-19 was in such place. Failure to do so may subject the employer to a fine of up to THB 20,000.
Are there any other noteworthy restrictions or conditions?	Only public health authorities, National Broadcasting and Telecommunications Commission (NBTC) and mobile phone service providers may access data in the contact tracing application.

Collecting COVID-19 Data



Can you collect health data for the purpose of COVID-19 response measures?	Yes.
What types of data can you collect?	“Necessary” data. This includes name, address, mobile number, travel history, temperature.
Can you collect social media data?	No.
What do you need to provide before you collect the data?	<p>Notify persons that the collection, use or disclosure of personal data is for purposes of being in compliance with the law, e.g. for purposes of contact tracing and other necessary response measures to contain the outbreak of COVID-19. The existing privacy notice may cover such data (although unlikely).</p> <p>A person’s personal data can only be processed without consent where the employee has contracted the Coronavirus, and the processing of their personal data is necessary to prevent secondary infection, and to continue business activities.</p>
Can you share the data?	<p>Yes – <u>if the person has been infected with COVID-19</u>, in the following circumstances:</p> <ul style="list-style-type: none">• within the company;• partners/other businesses to prevent secondary infection, to continue business activities at the business partner, or to enhance public hygiene; and• where a public health center has decided to provide a business operator with the work history of the employee, no consent is required to provide that information.
How must you protect the data?	Businesses should consider carefully the scope of personal data to be transferred and the number of people receiving the personal data.
What if an employee has COVID-19?	The infected individual’s consent is not required for (i) sharing his personal data within the company; (ii) with the employer’s business partner, even if it exceeds the scope of utilization purpose originally specified, in order to prevent secondary infection and to continue business activities at the business partner. Where a public health center has decided to provide a business operator with the work history of the employee, no consent is required to provide that information.
How long can you retain the data?	Data should be deleted without delay when they are no longer necessary for the processing purposes to avoid unnecessary retention of data.

Contact Tracing & Reporting



Is there a contact tracing application or program available?	Yes – COCOA (Contact-Confirming Application).
Is use of a contact tracing application mandatory?	No.
What data must be reported to the relevant authority/government department?	Contact tracing app data. Note: the app does not collect the names, phone numbers or geolocation data, but uses pseudonymous data.
Are there any other noteworthy restrictions or conditions?	When providing or receiving personal information to or from a third party, employers must maintain records of personal data transferred or received, including the name and address of the receiving or transferring third party.

Collecting COVID-19 Data



<p>Can you collect health data for the purpose of COVID-19 response measures?</p>	<p>Yes.</p>
<p>What types of data can you collect?</p>	<p>Information “necessary” to prevent infectious diseases, includes names, resident registration numbers, addresses, phone numbers, travel history, temperature.</p>
<p>Can you collect social media data?</p>	<p>No.</p>
<p>What do you need to provide before you collect the data?</p>	<p>Notify persons that the collection, use or disclosure of personal data is for purposes of being in compliance with the law, e.g. for purposes of contact tracing and other necessary response measures to contain the outbreak of COVID-19. The existing privacy notice may cover such data (although unlikely).</p> <p>Government agencies that require personal data for public interest purposes can collect and use data without the need to obtain consent.</p>
<p>Can you share the data?</p>	<p>Yes – <u>if there is a suspected case</u>, to immediately report to the public health center. <u>if the person has been infected with COVID-19</u>, to immediately inform all workers of the fact. An employer can only share minimum information needed in securing the general health and safety of other employees (e.g. where the infected personnel visited, date when it occurred would likely be permissible).</p>
<p>How must you protect the data?</p>	<p>Employers must protect the employee’s right to privacy of their medical data and use such data to a minimum extent.</p>
<p>What if an employee has COVID-19?</p>	<p>See above.</p>
<p>How long can you retain the data?</p>	<p>Data should be deleted after being utilized for the purposes collected (however note that the South Korea government admitted that it is permanently keeping data on patients from the previous MERS epidemic)</p>

Contact Tracing & Reporting



Is there a contact tracing application or program available?	Yes – government app. Note there are also other apps available, e.g. another government app providing a public database of detailed information about infected individuals, including their movements around the country.
Is use of a contact tracing application mandatory?	Yes – those arriving at the airport must download a government mobile app that tracks their location and asks them to report any symptoms.
What data must be reported to the relevant authority/government department?	Where there are suspected cases in the workplace, this should immediately be reported to the public health center or KCDC call center, who will request the necessary information.
Are there any other noteworthy restrictions or conditions?	Public agencies including the Ministry of Health and Welfare (MOHW) and Korea Centers for Disease Control and Prevention (KCDC) -- <u>7 categories of data of infected persons</u> : location data (including location data collected from mobile devices); personal identification information; medical and prescription records; immigration records; card transaction data for credit, debit, and prepaid cards; transit pass records for public transportation; and closed-circuit television (CCTV) footage.



LATHAM & WATKINS LLP

Questions?

MCLE

Record this code now:

3106230

All participants will need to record this code on the MCLE Record of Participation form to receive MCLE credit for viewing this programme.

Contact Information



Kieran Donovan

Hong Kong

Email: kieran.donovan@lw.com

Phone: +852.2912.2701



Gen Huong Tan

Singapore

Email: genhuong.tan@lw.com

Phone: +65.6437.5349