DPEX

DATA PROTECTION EXCELLENCE NETWORK

MOBILE APPLICATION PRIVACY SWEEP

Review of Singapore's TraceTogether App

Abstract

This is a privacy review of the mobile application TraceTogether, applying GPEN's privacy sweep methodology as well as the 9 obligations of Singapore 's Personal Data Protection Act and

Kevin Shepherdson & Lyn Boxall

STRAITS INTERACTIVE

CONTENTS

1.0 Introduction

On 21 March 2020, the Government of Singapore launched its 'TraceTogether' mobile application. It was developed by the Ministry of Health (MOH) and Government Technology Agency of Singapore (GovTech) in support of SGUnited. (SGunited is a portal to help Singaporeans support COVID-19 efforts. It was launched by the Social and Family Development Minister on 20 February 2020.) The TraceTogether app can be downloaded and used by anyone with a Singapore mobile number and a Bluetooth-enabled smartphone.

We have heard a lot about how technologies used to help manage the COVID-19 outbreak may threaten the privacy of individuals and communities. So, this is what we did:

- In 2014, 25 privacy enforcement authorities around the world participated in a global privacy sweep - that is, a survey - of mobile apps organised by the Global Privacy Enforcement Network (GPEN). (View the full report here.) In total, they assessed 1,211 apps, looking at the types of permissions (and, therefore, personal data each app was seeking), whether those permissions exceeded what would be expected based on the app's functionality and, most importantly, how the app explained to consumers why it wanted the personal data and what it planned to do with it We benchmarked the TraceTogether app against these GPEN survey parameters. This included reviewing the privacy statement in the app and comparing it with the permissions requested by the app when a user downloads it.
- We applied the nine obligations under the Personal Data Protection Act (PDPA) to the privacy statement in the TraceTogether app - even though GovTech and MOH are not required to comply with the PDPA - and assessed compliance by the TraceTogether app with each of those obligations.
- We applied the processing principles under the General Data Protection Regulation (GDPR) to the TraceTogether app - again, even though the GDPR does not apply to it - and assessed its consistency with those principles.

2.0 Executive Summary

In summary, we found that:

1. In terms of benchmarking against the GPEN survey parameters, the types of permissions sought by the TraceTogether app do not exceed what would be expected based on the app's functionality and, with one exception, explains clearly why it wants specific information and what will be done with it.

2. The exception concerns location data permissions. The developers could have proactively clarified potential confusion arising from a technical need to seek this permission against the practicality that location information is not collected or stored by the TraceTogether app.

3. The privacy statement and accompanying documents explain clearly and in simple English (that is, not in legalese) what the TraceTogether app does, what kind of personal data is collected and how it may be used or disclosed. Our review shows that the permissions the app seeks do not exceed its functionality and declared purposes.

4. The TraceTogether app does not comply with all of the nine obligations under the PDPA or all of the six principles under the GDPR, but is generally consistent with those obligations and principles. The few areas where it falls short tend to reflect the nature of an app such as the TraceTogether app rather than an inadvertent or careless departure from an obligation or principle.

The way the TraceTogether app works technically is described in some detail below. Our analysis that leads to us reaching the above summarised conclusions then follows.

PRIVACY COMMUNICATIONS	TraceTogether
Apps with concerns regarding pre-installation privacy communications	NA
Apps with excessive permissions based on sweeper's understanding of app's functionality	NA
Apps with privacy communications not well tailored to small screen	NA

OVERALL PRIVACY MARKS	TraceTogether
0 = No privacy information, other than permissions	NA
1 = Privacy information not adequate; sweeper does not know how information will be collected, used and disclosed	NA
2 = Privacy information somewhat explains the app's collection, use and disclosure of personal information; however, sweeper still had questions about certain permissions	NA
3 = Privacy information clearly explains how app collects/uses/discloses personal information; sweeper is confident in his/her knowledge of app's practices	Yes

PERMISSION REQUESTED	TraceTogether
Location	Yes
Photos/Media/Storage	Yes
Contacts	-
Calendar	-
Microphone	-
Camera	-
Device ID	-
Access to other accounts	-
SMS	-
Call log	-

3.0 Background

3.1 Objectives of the TraceTogether app

The objectives of the TraceTogether app are to:

- allow users to 'proactively help' in contact tracing (by downloading the app and consenting to participate in the contact tracing process) and
- support ongoing COVID-19 preventative efforts by speeding up and simplifying contact tracing while simultaneously making it more thorough

Contact tracing is identifying and following-up individuals who may have come into contact with an individual infected with COVID-19 to help them get relevant care and treatment.

3.2 How the TraceTogether app works

When a user downloads the TraceTogether app they register their mobile phone number and the app assigns a random anonymised User ID to the user's mobile phone to identify it uniquely - 9I8VPeQeWDofj39c8dPySoUXLqh2, for example.

The only personal data stored by GovTech (as developer of the TraceTogether app) is the mobile phone number and the User ID. These are stored in a secure server and are never disclosed to the public.

After being downloaded, the app works as follows:

- A Temporary ID is generated by encrypting the User ID. It can be decrypted only by MOH. The Temporary ID does not reveal the identity of the user of the app. The Temporary ID is refreshed at regular intervals. The lack of a persistent identifier means it is impossible for third parties to identify a user of the app or to track them.
- The user's mobile phone uses short-distance Bluetooth signals to exchange the Temporary ID of their mobile phone with the Temporary ID of any other user of a mobile phone on which the TraceTogether app has been downloaded whenever the two

phones are in 'close proximity'. Current MOH guidelines define 'close proximity' as two metres apart or up to five metres for 30 minutes.

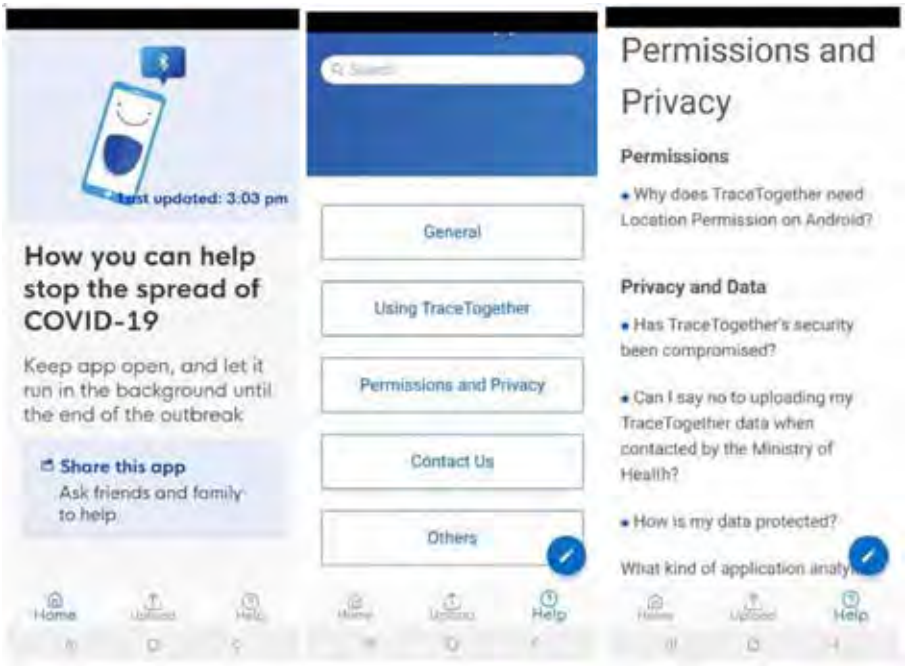
- The 'close proximity' information is stored in the mobile phone of a TraceTogether app user for 21 days on a rolling basis. When the information is 21 days old it is automatically deleted from the user's mobile phone by the TraceTracker app.
- If:
  - o a user of the TraceTogether app falls ill with COVID-19 or
  - o the mobile phone of a user of the TraceTogether app is found to have been in 'close proximity' with a mobile phone where contacts need to be traced (because the user of the TraceTogether app was in 'close proximity' with a COVID-19 case),

  MOH decrypts the user's Temporary ID, revealing their User ID to MOH. At this stage, the user's phone number is also disclosed to MOH so that the individual can be contacted to enable contact tracing.
- MOH will seek the user's consent to share their 'close proximity' information for the past 21 days with MOH. This is the only time users will be asked to share the 'close proximity' information.

  When an individual is contacted by MOH they are required by law to assist in contact tracing irrespective of whether the individual uses the TraceTogether app. If they refuse to do so they may be prosecuted under the Infectious Diseases Act. The objective of MOH seeking consent to using 'close proximity' information collected by the TraceTogether app is to make it quicker for MOH to contact people who have had close contact with the infected individual.

3.3 Privacy Statement

Prior to a user deciding to download the TraceTogether app, GovTech makes an effort to explain clearly what the app does, what kind of personal data will be collected and how it may be used and disclosed. You can view the privacy statement here.



In addition, *within the app*, there is a help button that lists useful information about "Permissions and Privacy". This is provided in a Q&A format, which explains what is stated in the privacy policy and proactively addresses many privacy concerns of users.

4.0 Benchmarking the TraceTogether app against the GPEN survey parameters

4.1 Methodology

As mentioned above, in 2014 GPEN did a global privacy sweep that assessed:

- the types of permissions sought by mobile apps: this means that the assessed the categories of personal data each app was seeking
- whether those permissions exceeded what would be expected based on the app's functionality: for example, an app might seek permission to use location data from the user's mobile phone, which means it has information about the user's location and physical movements and
- v most importantly, how the app explained to consumers why it wanted the personal data and what it planned to do with it: for example, an app provided by a bank might seek location data so it can alert the user to nearby ATMs.

To understand this, we will first take a look at app 'permissions' generally.

4. 2 About App Permissions

A 'permission' in an app protects the privacy of the user of the app. Every app must include 'app manifest' that, amongst other things, lists the permissions that the app uses.

Every mobile phone has an 'operating system, most commonly the Android operating system (Google) or the iOS (Apple) operating system. The vast majority of mobile phones are 'Android phones' and they have two 'permissions' categories:

- *Normal permissions:* these permissions do not directly risk the user's privacy - for example, permission to set the time zone is a normal permission. If an app lists a normal permission in its manifest, the system grants the permission automatically.

- *Dangerous permissions:* these permissions give the app access to the user's personal data in their mobile phone, such as contacts and SMS messages, as well as certain system features, such as the camera. If a dangerous permission is requested, privacy laws do not allow the relevant personal data to be collected, used or disclosed unless the user gives explicit consent by 'accepting' the request for permission to do so. In addition, privacy laws generally restrict 'dangerous permissions' to personal data that the app may collect, use or disclose while the user is actually using it - they do not allow apps to collect, use or disclose personal data simply because the user downloaded the app.

By way of illustration, here is a list of dangerous permissions that might be sought by an app:

PERMISSION GROUP	PERMISSIONS
Calendar	• READ_CALENDAR • WRITE_CALENDAR
Camera	• CAMERA
Contacts	• READ_CONTACTS • WRITE_CONTACTS • GET_ACCOUNTS
Location	• ACCESS_FINE_LOCATION • ACCESS_COARSE_LOCATION
Microphone	• RECORD_AUDIO
Phone	• READ_PHONE_STATE • CALL_PHONE • READ_CALL_LOG • WRITE_CALL_LOG • ADD_VOICEMAIL • USE_SIP • PROCESS_OUTGOING_CALLS
Sensors	• BODY_SENSORS
SMS	• SEND_SMS • RECEIVE_SMS • READ_SMS • RECEIVE_WAP_PUSH • RECEIVE_MMS
Storage	• READ_EXTERNAL_STORAGE • WRITE_EXTERNAL_STORAGE

Here are the permissions sought by the TraceTogether app. You can view the permissions here (scroll to the end and view details in "Permissions") when it is downloaded to an Android phone.

Dangerous: Photos/Media/Files	• read the contents of your USB storage • modify or delete the contents of your USB storage
Dangerous: Storage	• read the contents of your USB storage • modify or delete the contents of your USB storage
Dangerous: Location	• approximate location (network-based) • precise location (GPS and network-based)
Normal	• receive data from the Internet • access Bluetooth settings • full network access • prevent device from sleeping • view network connections • pair with Bluetooth devices • run at startup

We looked at whether these dangerous permissions exceeded what would be expected based on the TraceTogether app's functionality. We also looked at the explanation in the TraceTogether's privacy statement about why these permissions are needed and what will be done with the relevant personal data.

4.3 Photos/Media/Files/Storage

We can see that TraceTogether seeks permission to:

- modify or delete the contents of the USB storage in a user's mobile phone
- read the contents of a user's USB storage in their mobile phone

These permissions are sought so that the app can store 'close proximity' information for 21 days on a rolling basis (as described above under 'How the TraceTogether app works'), and so that the 'close proximity' information can be read if it becomes necessary to trace the user's contacts.

(An Android mobile phone has three types of storage (or memory): two of them are on a hard drive inside the phone; the third is on a separate memory card that the owner of the mobile phone may choose to purchase and use. The USB storage is a partition of the internal hard drive that comes with the phone - for example, where it is advertised that 'this phone has 16GB of memory' or 'this phone has 64 GB of memory'. It is the place where photos, media and files are stored. In the case of the TraceTogether app, it is the place where the 'close proximity' information is stored.)

The privacy statement in the TraceTogether app says that:

> 'Data about phones near you is stored only on your phone. If a user gets infected with COVID-19, he/she has the option to give MOH access to his/her TraceTogether data.'

and:

> 'When you grant MOH access to your TraceTogether data, this data will be used solely for contact tracing of persons possibly exposed to COVID-19.'

If MOH contacts a user of the TraceTogether app as part of contact tracing, MOH will ask the user to give them the 'close contact' information in the USB storage in their mobile phone. If the user agrees to do so, the app will read the contents of that USB storage and send it to the developer, GovTech. GovTech will send it to MOH.

4.4 Location

According to the privacy statement for the TraceTogether app:

> 'TraceTogether uses Bluetooth to approximate your distance to other phones running the same app. We do not collect data about your GPS location. Neither do we collect data about your WiFi or mobile network.'

The statement about location is inconsistent with the permissions listed above, namely:

- approximate location (network-based)
- precise location (GPS and network-based)

for which consent is sought by the app when downloading it.

This inconsistency arises because location permissions are mandatory when Bluetooth technology is used on an Android phone. It is an outcome of how the Bluetooth technology works - the location permission is required so that 'close proximity' information can be collected.

However, we can confirm that the app does not collect and store the location data used in relation to the 'close proximity' information. Neither the privacy statement nor the help documentation make this clarification, which could be confusing to a non-technical user.

5.0 Reviewing the TraceTogether App against the Nine Obligations in the PDPA

The Personal Data Protection Act, the PDPA, does not apply to the TraceTogether app because it is issued by a public agency. Public agencies are excluded from the scope of the PDPA, including because they are required to abide by their own internal rules that are said to be similar to the PDPA but that are not available to the public. Because of that non-availability, we review the TraceTogether app against the nine obligations in the PDPA on the basis that it represents 'best practices' in data protection in Singapore.

5.1 Consent Obligation and Notice Obligation

Obtaining Consent

The PDPA provides that an organisation must not collect, use or disclose personal data about an individual unless the individual has consented (or is deemed to have consented), unless such collection, use or disclosure without consent is authorised by the PDPA or any other written law. The organisation must notify the individual of the purpose of such collection, use or disclosure before seeking their consent.

1. First, when **downloading** the TraceTogether app and setting it up so that it will work, the user needs to provide consent for 'push notifications'.

   A push notification is a message that can be sent by GovTech (as provider of the TraceTogether app) to the user's mobile phone at any time after they have downloaded that app. The user does not have to be in the app or even using their mobile phone when a push notification is sent to them. The user will see it the next time they use their mobile phone.

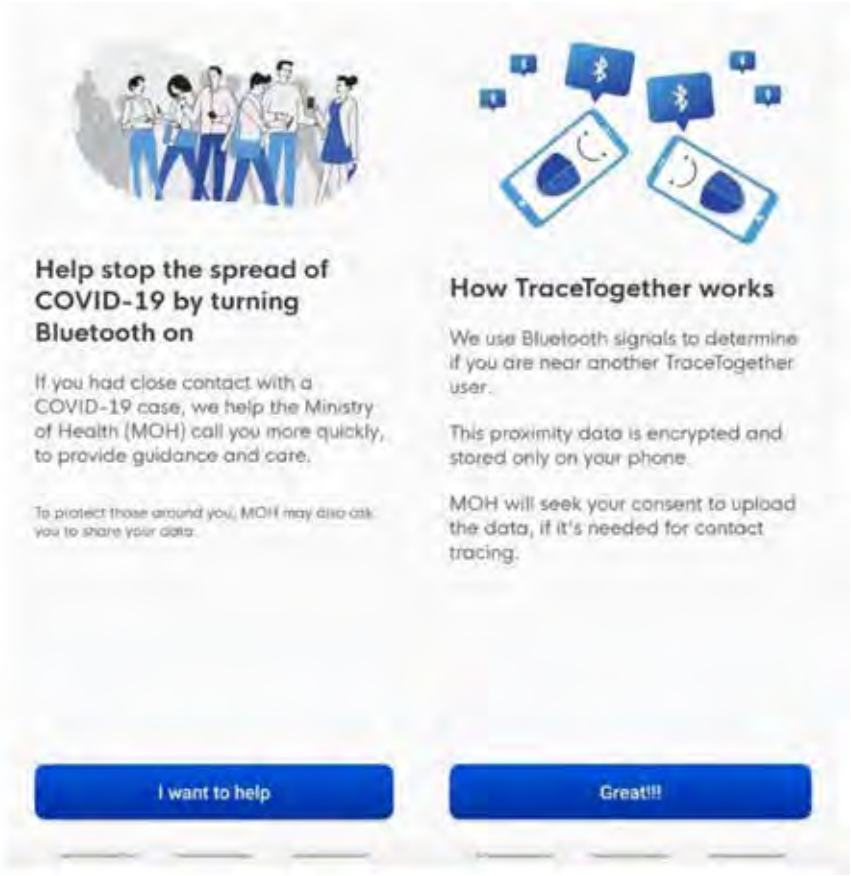
   The ability for a user to receive a push notification in connection with the TraceTogether app is so that the user of the app can be alerted for contact tracing purposes or, once contact tracing ceases, to prompt the user to disable the app.

   This is not mentioned in the privacy statement for the TraceTogether app; nor is it explained clearly in the accompanying materials.

Instead, it is assumed that individuals downloading the app will understand why they are consenting to push notifications.

2. Second, when **downloading** the TraceTogether app and setting it up so that it will work, the user needs to provide consent for the app to track the location of the mobile phone. As discussed above, this permission is necessary in an Android phone so that the Bluetooth technology will work. The app does not collect or store location information.

3. Third, when **downloading** the TraceTogether app and setting it up so that it will work, the user needs to turn on the Bluetooth function on their phone. This is required so that the Bluetooth technology can generate 'close proximity' information that it will store in the user's mobile phone.



These screenshots show that a user gives their consent when they hit: "I want to help"

This complements the privacy statement that is viewable both *prior to download* and *within the app* after download - a help button provides a Q&A on 'Permissions and Privacy'.

The TrackTogether app's privacy statement says:

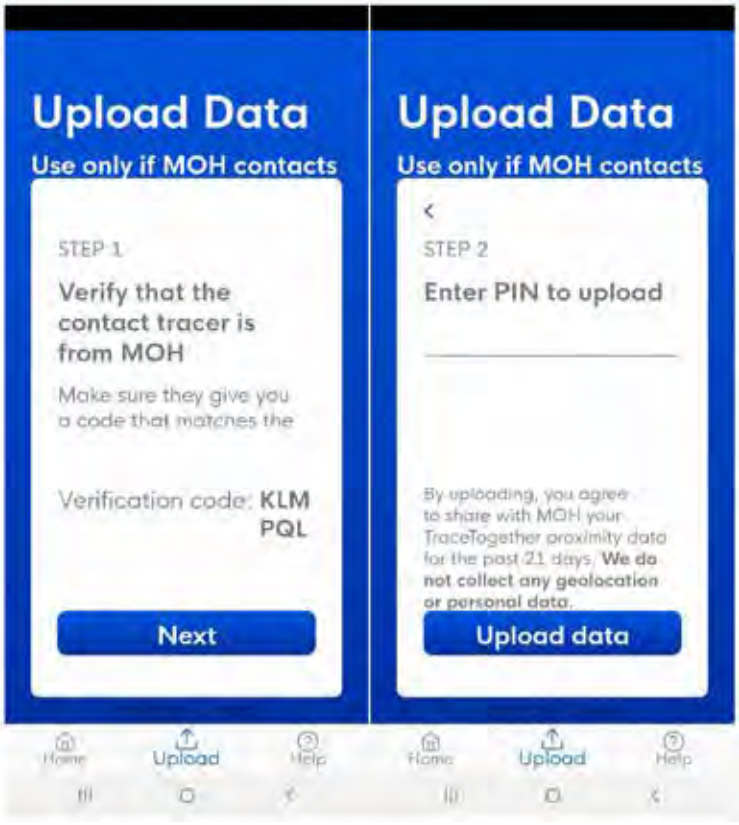
> 'With your consent, [the app] exchanges Bluetooth signals with nearby phones running the same app. This allows you to be informed if you were in prolonged physical proximity with an infected person.'

and:

> 'When you are close to another phone running TraceTogether, both phones use Bluetooth to exchange a Temporary ID …'

In summary, the user is notified of the purposes for which the TraceTogether app will collect 'close proximity' information and gives consent to it exchanging information with other mobile phones running the TraceTogether app in order for the app to do so.

4. Fourth, after the user has downloaded the TraceTogether app and used it they may be contacted for contact tracing purposes. The following screenshots show what happens when MOH wants to do contact tracing using 'close proximity' information:



Users will only be asked to consent to share 'close proximity' information stored in their mobile phone (by hitting the upload button) if they have been in contact with a COVID-19 infected individual.

Consequently, we conclude that GovTech and MOH have complied with the consent obligation and the notification obligation in each of the four situations discussed above, albeit with a minor reservation in connection with consent for 'push notifications'.

Excessive Collection of Personal Data

Under the PDPA, consent given by an individual is not valid if the personal data to be collected, used or disclosed is beyond what is reasonable to provide relevant products or services to that individual.

As discussed above, our analysis of the privacy statement and the permissions sought by the TraceTogether app shows that it collects, uses and discloses personal data only to 'facilitate the contact tracing process'. The app makes a very conscious effort to collect only minimal information that is relevant to contact tracing. Other than the mobile phone number, the TraceTogether app does not collect any other contact information whatsoever. Therefore, we conclude that it does not collect excessive personal data.

Withdrawing Consent

Under the PDPA, an individual may upon giving reasonable notice, withdraw any consent given (or deemed to have been given) to the collection, use or disclosure of personal data about them.

The privacy statement for the TraceTogether app says that the consent to collect 'close proximity' information can be revoked at any time:

> 'You can revoke consent by emailing support@tracetogether.gov.sg with the mobile number you registered in the app.
>
> We will then delete your mobile number and User ID from our server. This renders meaningless all data that your phone has exchanged with other phones, because that data will no longer be associated with you.'

Logically, there is no sense in an individual trying to withdraw the consent given to MOH uploading the 'close proximity' information from their phone as this upload would be done immediately after the user hits 'Upload data' (which action also provides MOH with the consent to do so). In any event, it is far from clear that 'close proximity' information would, in any event, be personal data.

Therefore, we conclude that GovTech and MOH have complied with the requirements under the PDPA to allow individuals to withdraw consent to the collection, use or disclosure of personal data about them.

5.2 Purpose Limitation Obligation and Notification Obligation

Under the PDPA, an organisation may collect personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and that have been notified to the individual.

GovTech and MOH might have chosen to collect information about the specific location of users of the TraceTogether app when they were in 'close proximity' to an individual who is subsequently found to be infected with COVID-19. They might have chosen to collect the mobile phone numbers of such individuals. This information might have been useful, for example, in identifying and analysing clusters of infection. However, GovTech and MOH have specified a more limited purpose and have taken care to restrict the collection, use or disclosure of personal data by the TrackTogether app to that specific purpose of which they notify users.

Consequently, we conclude that the TraceTogether app complies with the Purpose Limitation Obligation and the Notification Obligation under the PDPA.

5.3 Access and Correction Obligation

The PDPA gives individuals a right to have access to their personal data - that is, to find out what personal data an organisation holds about them - and a right to find out how it has been, or may have been, used or disclosed in the previous year. They also have a right to correct any error or omission in such personal data.

The TraceTogether app does not give an option for the user to obtain access to their personal data, to be told how it may have been used or disclosed within the previous year or to correct it. This is unnecessary given that the only piece of personal data collected by the app is the mobile phone number that the user registers for the purpose of using the app and how it may be used or disclosed is stated clearly in the privacy statement and related documentation.

If the user changed their mobile phone number they could simply download the TraceTogether app again and register their new phone number in connection with it.

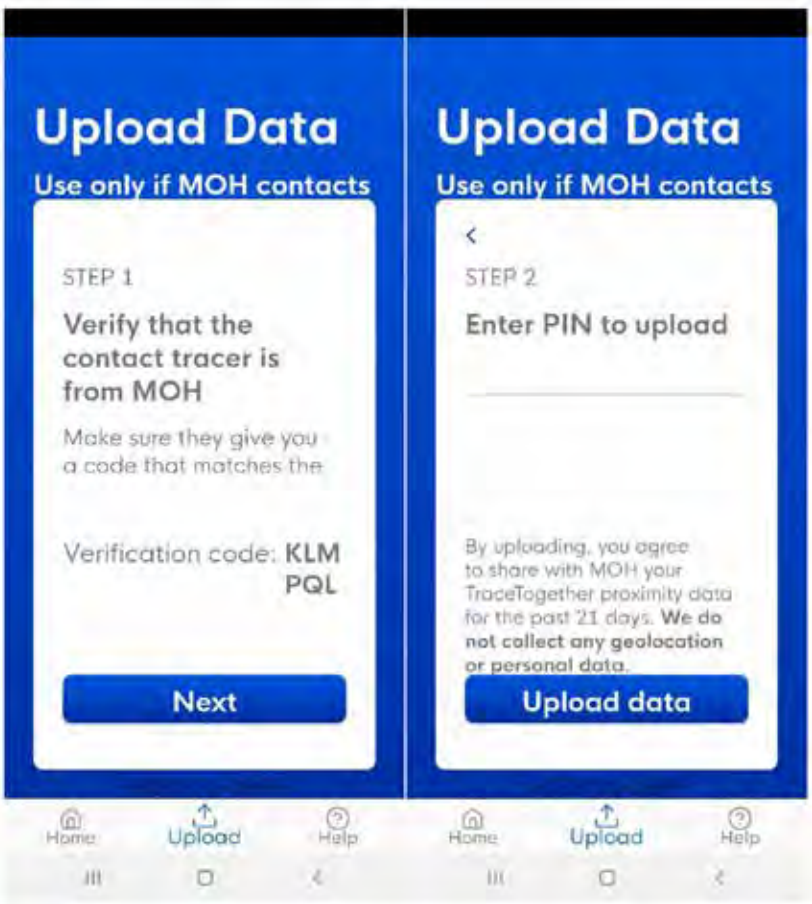
5.4 Accuracy Obligation

The PDPA requires an organisation to make a reasonable effort to ensure that personal data is accurate and complete if it is likely to be used to to make a decision is likely to be disclosed to another organisation.

The TraceTogether app verifies the user's mobile number with two-factor authentication using a One-Time Pin (OTP) sent to the mobile phone number provided by the user of the app:

- During registration process
- When user is asked to upload information) when contacted by MOH)

and we conclude that, in the circumstances, this is a reasonable effort to ensure accuracy.



5.5 Protection Obligation

The Protection Obligation requires an organisation to protect personal data by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

The privacy statement for the TraceTogether app assures users that:

> 'both the mobile number and User ID are stored in a secure server, and never shown to the public'

and that a set of cryptographically generated temporary IDs are used so that, as stated in the in the help documentation for the app:

> 'mobile numbers are not revealed to other TraceTogether users'

That documentation also explains that:

> 'the data collected is stored locally in the user's phone in an encrypted form. The data will never be accessed, unless the user has been in close contact with a COVID-19 case and is contacted by the contact tracing team'.

The TraceTogether app uses public/private key encryption (PKI), as explained in the privacy statement:

> 'This Temporary ID is generated by encrypting the User ID with a private key held by the Ministry of Health (MOH). It can only be decrypted by MOH, and does not reveal your identity or the other person's identity.'

Finally, if there is contact tracing involving the user, the screenshot above shows that the user is asked to first:

> 'verify if the contact tracer is from MOH". In addition, a PIN is required as further evidence of validation and accuracy prior to the user uploading the required data from the application.

We conclude that each of these elements are reasonable security arrangements to protect personal data and that, therefore, the TraceTogether app satisfies the protection obligation under the PDPA.

5.6 Retention Limitation Obligation

The PDPA requires an organisation to cease to retain its documents containing personal data as soon as it is reasonable to assume that it is no longer needed for legal or business purposes. Alternatively, an organisation may anonymise the personal data.

As to the mobile phone number collected when the TraceTogether app is downloaded:

- At least by implication, given the stated purpose of the Trace Together app, the user's mobile phone number will be retained by GovTech, as developer of the app, for as long as COVID-19 epidemic measures require contact tracing. This is supported by the privacy statement saying that:

  'Once contact tracing ceases, you will be prompted to disable TraceTogether's functionality.'

- its privacy statement also says that:

  'You can revoke consent by emailing support@tracetogether.gov.sg with the mobile number you registered in the app.

  We will then delete your mobile number and User ID from our server. This renders meaningless all data that your phone has exchanged with other phones, because that data will no longer be associated with you.'

As to the 'close proximity' information that is collected by the TraceTogether app, as mentioned above the app documentation says that it is deleted on a rolling 21 days basis. Whether the code is written in such a way that the 'close proximity' information is automatically purged after 21 days (versus being archived) is unknown.

In addition, the privacy statement says that:

'The Temporary ID … is refreshed at regular intervals.'

In summary, GovTech will hold the mobile phone number of a user of the TraceTogether app until the user revokes their consent or disables the app. This puts control in the hands of the user and reflects the reality that GovTech will not know if a user simply decides to stop using the app, even if they uninstall it. The time for which elements of data collection that are within the control of GovTech are retained

- namely, the User ID and the 'close proximity' information - is limited by the design of the app to disposal at 'regular intervals' and '21 days', respectively.

Overall, it is not possible to state with any degree of certainty that the TraceTogether app complies with the retention limitation obligation under the PDPA. However, it seems that GovTech and MOH have done everything possible in designing the app to ensure that personal data will not be retained when it is no longer necessary for contact tracing purposes.

5.7 Transfer Limitation Obligation

The transfer limitation obligation imposes rules on organisations if they send personal data outside of Singapore. There is nothing in the privacy statement for the TraceTogether app or in the documentation that accompanies it to suggest that personal data is sent outside of Singapore. Therefore, we have concluded that the transfer limitation obligation is not relevant to the TraceTogether app and the personal data that it collects, uses or discloses.

5.8 Openness / Accountability Obligation

Openness under the PDPA requires an organisation to make information available about the manner, and the purposes, for which it collects, uses or discloses personal data. Accountability requires an organisation to take responsibility for its actions in a proactive way. In our review, we have concluded that the TraceTogether app satisfies both aspects of this final obligation, including through the information provided in the privacy statement and accompanying documents and in the way the TraceTogether app has been designed.

6.0 Comparing the TraceTogether app with the GDPR processing principles

It is clear that the General Data Protection Regulation, the GDPR, does not apply to the TraceTogether app. However, the GDPR is considered in some quarters to be the 'gold standard' in data protection. Consequently, we decided to compare statements made in the privacy statement for the TraceTogether app and the accompanying documents with the processing principles set out in the GDPR.

(Before reading the various principles, please refer to the elaborations in the previous section as reference)

6.1 Lawfulness, Fairness and Transparency Principle

The GDPR states that 'personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject'.

'**Lawfulness**' means that there needs to be a legal basis for processing the personal data. This does not quite 'translate' across to a PDPA environment, because the PDPA is consent based whereas the GDPR is not. However, consent is one of the six lawful bases for processing under the GDPR. It is clear from the discussion above, that the TraceTogether app satisfies the requirements for consent being given by the user / data subject.

Another of the six lawful bases for processing under the GDPR is where processing is 'necessary in order to protect the vital interests of the data subject or another natural person'. Both the European Data Protection Board (in connection with the GDPR) and the Personal Data Protection Commission of Singapore (in connection with the PDPA) have issued confirmation that preventative measures for COVID-19 fall within this lawful basis of processing personal data.

In any event, we conclude that the TraceTogether app satisfies the requirement of lawfulness because it seeks the user's consent to personal data about them being processed for the purposes of the app.

The GDPR contains certain rules that are stated to be necessary to ensure '**fair**' and '**transparent**' processing of personal data. They are stated below, together with our comments about whether or how the TraceTogether app satisfies them:

- the period for which the personal data will be stored or, if that is not possible, the criteria used to determine that period - we have commented on this in relation to the retention limitation obligation under the PDPA and concluded that GovTech and MOH have done everything possible in the context of an app such as the TraceTogether app, except for making it clear whether or not 'close proximity' information is automatically purged (not archived) 21 days after it is collected
- the existence of the right to request access to personal data and the right to correct it (as well as various other rights that are relevant to the GDPR, but not to the PDPA) - we commented on this in the context of the corresponding obligation under the PDPA and concluded that it is not satisfied by the TraceTogether app, but also that there is no real context for satisfying it
- where consent is the lawful basis of processing, the existence of the right to withdraw consent - this is included in the privacy statement for the TraceTogether app
- the right to lodge a complaint with a supervisory authority - this is not included in the privacy statement for the TraceTogether app, which is not surprising given that the app is provided by two public agencies
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data - the TraceTogether app is positioned as a 'public service' opportunity for its users so there is no real scope for this rule to apply to it
- the existence of automatic decision-making, including profiling - so far as we are aware, this is not relevant to the TraceTogether app and, indeed, GovTech and MOH seem to have taken great care to limit the app to a single purpose, which is contact tracing

We conclude that, while not everything in the above list is satisfied by the privacy statement and other accompanying documents for the TraceTogether app, overall it does collect personal data fairly and is transparent about how it will be processed.

6.2 Purpose Limitation Principle

The GDPR states that personal data shall be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

We have considered the Purpose Limitation under the PDPA, which is substantially the same as the corresponding principle GDPR and concluded that it is satisfied by the TraceTogether app.

6.3 Data Minimisation Principle

The GDPR states that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

We considered the amount of personal data collected by the TraceTogether app under the heading of 'Excessive Collection of Personal Data' in connection with the Consent Obligation under the PDPA and concluded that it does not collect excessive personal data. However, it is not clear whether a requirement not to collect excessive personal data would satisfy the data minimisation principle under the GDPR - personal data collection might not be excessive, while still not being minimised.

However, we conclude that not only does the TraceTogether app not collect excessive personal data in light of its purpose, but does comply with the data minimisation principle under the GDPR.

6.4 Accuracy Principle

The GDPR states that personal data shall be accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

This principle corresponds with the Accuracy Obligation under the PDPA. We concluded above that the TraceTogether app satisfies it by sending an OTP in order to confirm the user's mobile phone number. We also conclude that the same process satisfies the Accuracy Principle under the GDPR.

6.5 Storage Limitation Principle

The GDPR states that personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

This principle corresponds with the Retention Limitation Obligation under the PDPA. We concluded above that the TraceTogether app does not satisfy the Retention Limitation Obligation literally, but that it does do so in light of the limitations imposed in the context of an app. We reach the same conclusion regarding the GDPR's Storage Limitation Principle.

6.6 Integrity and Confidentiality Principle

The GDPR states that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

This principle corresponds with the Protection Obligation under the PDPA. For the same reasons as set out in relation to the Protection Obligation, we conclude that the TraceTogether app satisfies the Integrity and Confidentiality Principle under the GDPR.

------The End------

About Straits Interactive

Straits Interactive delivers end-to-end governance, risk and compliance solutions that enable trusted business and responsible marketing, especially in the area of data privacy and protection. Recently Data Protection Trustmark (DPTM) certified, we help businesses achieve operational compliance and manage risks through a combination of cloud technology and professional services. Our quest for innovation has led to us being recognised and awarded Intercon's Top 50 Tech Companies (in recognition of the company's contribution to technology) and APAC Business Headlines' Company of the Year, 2019. Our software-as-a-service solutions include DPOinBOX and Governance, Risk & Compliance System (GRACIAs), all of which are supported by professional services that include advisory services, audits, and training. More information about the company can be found on www.straitsinteractive.com.

About the Data Protection Excellence (DPEX) Network

The Data Protection Excellence (DPEX) Network is the first of its kind facility in the ASEAN region whose aim is to provide leadership, best practices, training, research and support for all things surround data privacy from an operational perspective. This collaboration of partnerships comprise accreditation bodies, law firms, universities and organisations who provide professional services and technologies relating to data privacy. An ever-growing network, members currently include Straits Interactive, Singapore Management University, International Islamic University of Malaysia, De LaSelle University, Philippines, IAPP, EXIN, OCEG and Lexxion amongst others. More information about DPEX Network can be found at www.dpexnetwork.org