Privacy Impact Assessment for

LeaveHomeSafe Mobile App and related Support System (v3.0)

for OGCIO

Privacy Impact Assessment Report

Table of Contents

Change Control

The change control page will be used to record information for controlling and tracking modifications made to this document.

Version	Revision Date dd/mm/yyyy	Author(s)	Summary of Change(s)
1.0	02/11/2021	Contractor	All

Executive Summary

To faciliate the work of the Government in controlling the spread of COVID-19, a system, LeaveHomeSafe has been developed. The system are composed of 3 core components with enhacements: Exposure Notification Mobile App (the “mobile app”), Thematic Website and Admin Portal. A new function is developed to support the implementation of Hong Kong Health Code System (HCS).

Some personal information will be captured in each core component:

For the Mobile App

Users’ visit records are captured. This provides members of the public with a convenient digital tool for recording the time of their visits to different venues and taxi rides. The data including venue code, check-in timestamp, check-out timestamp, metadata with venue name, venue type and taxi registration mark are stored in the local database of the mobile app. All users’ visit records are encrypted and stored locally in their mobile devices for a retention period of 31 days. While visit records are encrypted in the mobile phones, as visit records can be viewed through the app, users should still protect their own personal devices against unauthorised access, in situations like stolen or lost mobile phones. Besides, users can download broadcast file for matching visit records of infected users. The records broadcast to app users contain no information that can be used to identify the users to whom the records belong.

In addition, there are some enhanced functions in different versions of the mobile app:

From version 3.0 onwards, registered users of HCS are able to upload their visit records and notification records to HCS after logging in their HCS account. The login information including identity document type, issuing country/region (if “Other identity document” type is selected”), identity document number and password will be sent to HCS for login authentication. An option is provided for users to remember the login information (except the password) and then fill in automatically to the login form next time. The login information is encrypted and stored locally in the users’ mobile devices.

Moreover, the app user tested with COVID-19 positive will be required to upload his/her visit records from the app to the LeaveHomeSafe server hosted in the Government Private Cloud.

For the Thematic Website

Contact information, venue type, supporting document number, supporting document file, venue area, venue district, venue name, and venue address are captured for venue QR code application.

For the Admin Portal

Notification broadcast, venue registration approval, account management, mobile app configuration managemnet and PIN managment are performed.

Furthermore, the personal data are securely protected in different states such as at rest and in transit with the use of data encryption. Also, different levels of access right are controlled based on the need-to-know principle. In addition, according to the Personal Data (Privacy) Ordinance (the "PDPO") Cap. 486, there is an exemption from some compliance requirements if the use of personal data is required for protecting a data subject’s health.

Overall, no issue or potential risk that may cause privacy data breach is identified after a detailed privacy impact analysis has been conducted.

Introduction

To provide members of the public with a digital tool to record the time of their visits to different venues so as to contain the spread of COVID-19, the LeaveHomeSafe exposure notification mobile app and related support system ("the System") have been implemented. A new function is developed to support the implementation of Hong Kong Health Code System (HCS).

This project is to conduct the Privacy Impact Assessment (PIA) and Privacy Compliance Audit (PCA) on the System for OGCIO of the Government of the Hong Kong Special Administrative Region (HKSARG or the Government).

Assessment Scope and Objectives

The Contractor has conducted PIA on the System to identify and address any data privacy implications / issues.

To conduct PIA according to the personal data privacy requirements under the Personal Data (Privacy) Ordinance (Cap. 486), the Contractor has been required to:

- study the current environment to recommend to OGCIO the following:
    - business and technical options to avoid or mitigate the identified actual or potential data privacy risks / implications / issues of the Systems, if any; *and*
    - measures to strengthen the security to safeguard the System from data privacy breaches, if any;
- be responsible for the total project management and act as a single contact point to OGCIO regarding all related activities of the PIA;
- take the lead in coordinating various parties within and outside the Government including other contractors of the Government for the smooth implementation of the PIA;
- resolve conflicts and crisis during the entire project life cycle;
- oversee and monitor the progress of various activities during the Contract Period to ensure that these activities are completed according to the implementation schedule while meeting the requirements of the Work Assignment Brief;
- plan and schedule meetings at appropriate time during the entire project life cycle, to prepare meeting agendas, and to take notes for all the meetings with various parties;
- report progress, follow up all outstanding issues with all related parties, suggest solutions and resolve problems throughout the PIA; *and*
- carry out any other activities which are necessary for the satisfactory completion of the PIA.

For the PIA, the Contractor has:

- performed data processing cycle analysis;
- performed privacy risks analysis;
- put forward recommendations or measures in avoiding or mitigating privacy risks; *and*
- compiled PIA report

and undertaken to:

- review and study the data collection, workflow, reports, documents, etc. of the System, in particular the current PICS and the content of notification being sent to the users;
- identify any privacy risks and issues with the System;
- identify the potential effects that the System may have upon personal data privacy;

- recommend safeguards based on the results of PIA in order to reduce the likelihood and impact of identified issues to an acceptable level;
- compile PIA report with recommendations on areas for improvement and hold presentations; *and*
- verify that all privacy issues identified in the PIA are properly addressed and safeguards to enhance privacy protection are implemented or slated to be implemented.

Assumptions and Limitations

All the information and documents in Technical Review that are collected from the representatives of the Contractor are treated as a trusted and legitimate source during the process of information gathering.

The PIA findings may vary, if there are any operational procedure changes / configuration changes in systems or applications in the future.

Reference Documentation

a. Security Regulations (SR)

b. Baseline IT Security Policy (S17)

c. The HKSARG Interoperability Framework (S18)

d. IT Security Guidelines (G3)

e. Guidelines on Application Software Testing (G20)

f. OGCIO IT Security Policy (OITSP)

g. Information Security Incident Handling Guidelines (G54)

h. Personal Data (Privacy) Ordinance (Cap. 486)

i. Electronic Transactions Ordinance (Cap. 553)

j. Practice Guide to Project Management for IT Projects under an Outsourced Environment (https://www.ogcio.gov.hk/en/infrastructure/methodology/proj_mgmt/pm_practice_guide_outsourced.htm)

k. Six Data Protection Principles issued by the Office of the PCPD

l. Code of Practice on the Identity Card Number and other Personal Identifiers issued by the Office of the PCPD

m. Technical Notes Pursuant to Chapter IX of the SR

n. The Government's Code of Access to Information

o. IoT Security Best Practice Guidelines

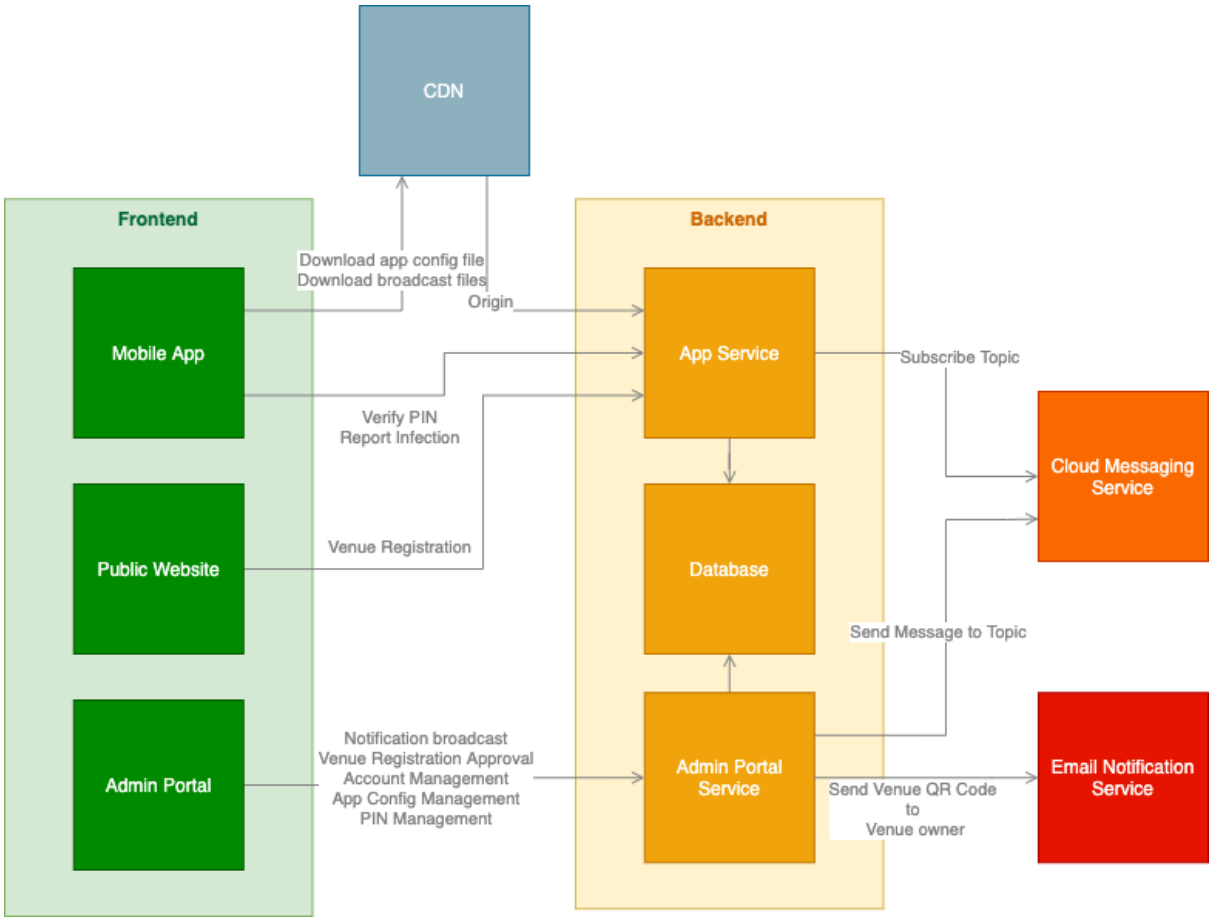
p. Any other related ordinances of the Government

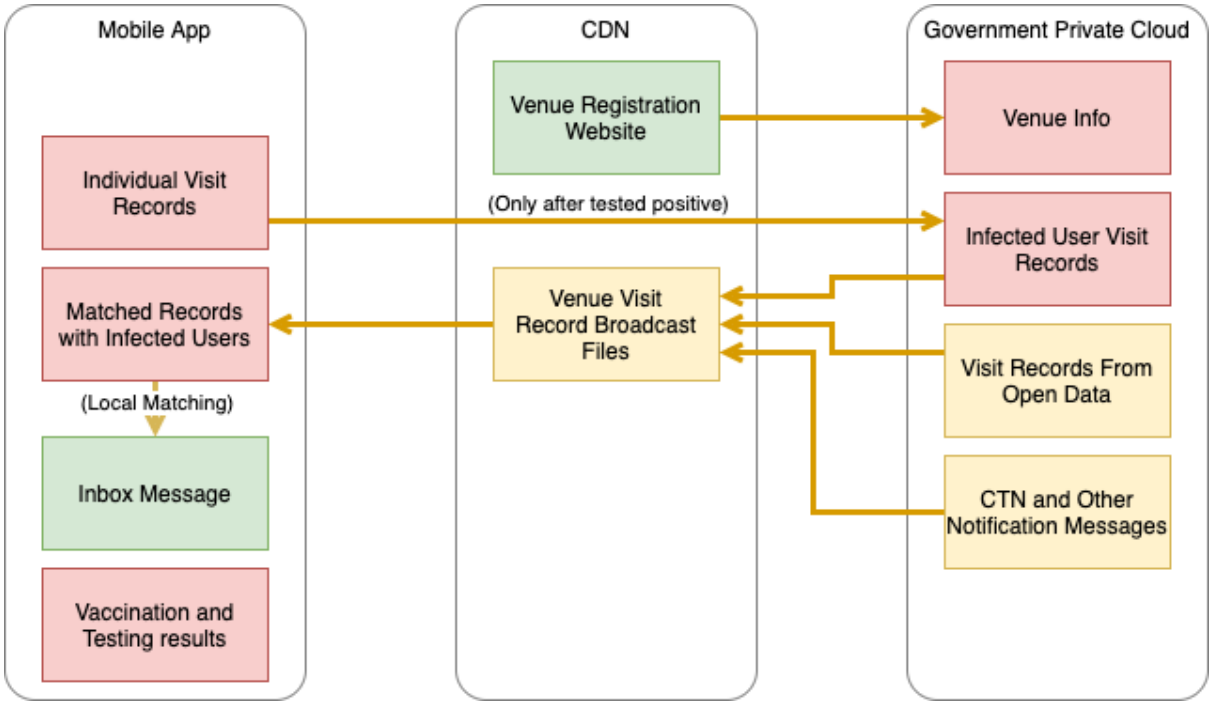
Consideration of Privacy Principle / Legislation and Policies

- The Personal Data (Privacy) Ordinance (the "PDPO") Cap. 486 :

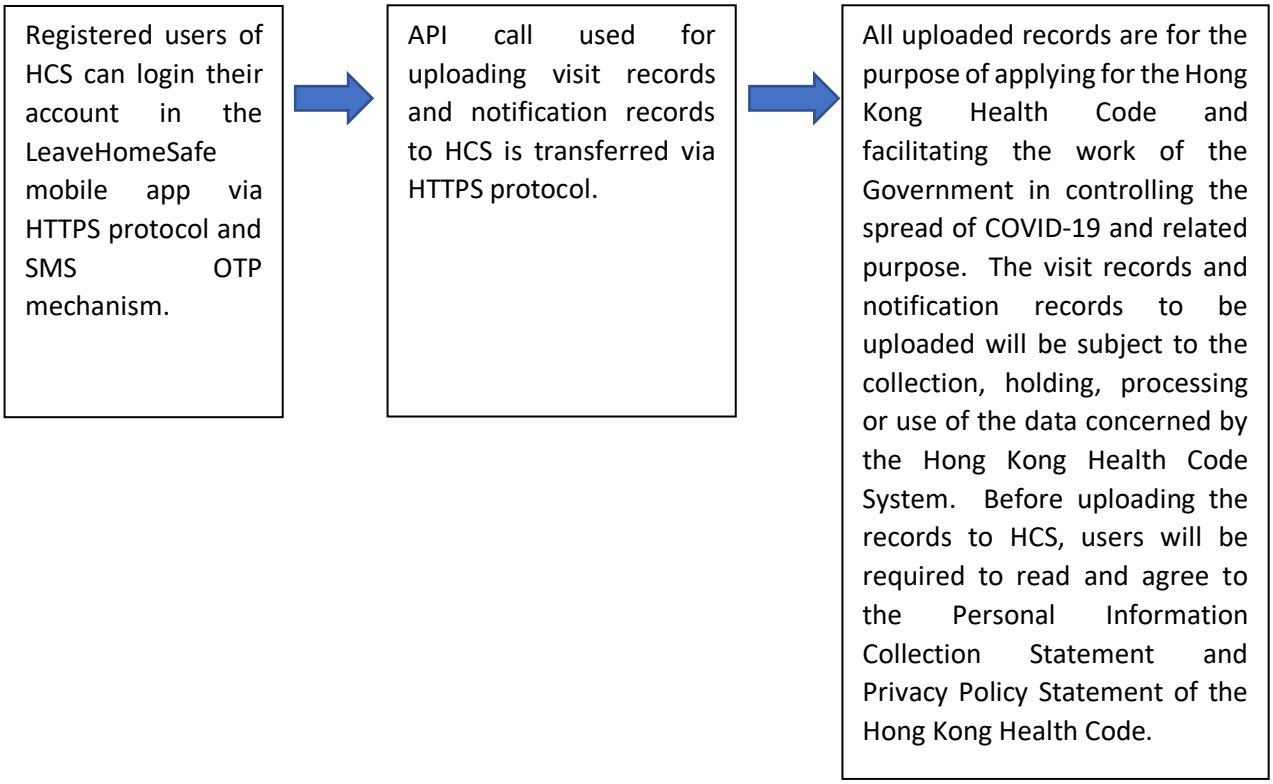
"Exemptions: While data privacy is an important right, the interests protected under PDPO have to be balanced against other important rights or public interest. PDPO provides a number of exemptions from some compliance requirements under particular circumstances. Examples include crime prevention or prosecution, security and defence, statistics and research, news activity, protecting a data subject's health etc. There is also an exemption if the use of personal data is required or authorised by law or court order or is required for exercising or defending legal rights in Hong Kong."

Description of Personal Information and Data Processing Cycle





New Function in Mobile App for Supporting the Implementation of Health Code System



Observed Security Measures Applied to Protect Personal Data

Data involved	Security Measures applied	Data Removal
Visit Records (in general situation)	Encrypted using AES-256 and stored in local mobile phones.	Automatically removed after 31 days.
Visit Records (for patients who are tested positive)	Encrypted using AES-256 and stored in local mobile phones. Required to be uploaded to LeaveHomeSafe servers in Government Private Cloud for epidemiological investigation with name and contact number by verification of PIN provided by CHP. All internet incoming traffic will be protected by HTTPS protocol.	Inside the app: Automatically removed after 31 days. Uploaded to CHP: Will be kept for at least 7 years by the Department of Health as with the same policy for other data for epidemiological investigations.
Visit Records and Notification Records for uploading to HCS (for registered users of HCS)	The API call used for uploading visit records and notification records to HCS is transferred via the HTTPS protocol. Only with their express consent, users may at their sole discretion upload their visit records and notification records from the LeaveHomeSafe mobile app to the Hong Kong Health Code System for the application of Hong Kong Health Code and its related purposes as well as facilitating the work of the Government in controlling the spread of COVID-19 and related purposes. The API call used for uploading visit records and notification records to HCS is transferred via the HTTPS protocol.	Uploaded to HCS: The visit records and notification records to be uploaded will be subject to the collection, holding, processing or use of the data concerned by the Hong Kong Health Code System. Please read and agree the Hong Kong Health Code System's Personal Information Collection Statement and Privacy Policy Statement before you proceed.
Venue registration information	LeaveHomeSafe servers in Government Private Cloud. All internet incoming traffic will be protected by HTTPS protocol.	Will be kept for 7 years or less when the data are no longer required.
Contact and enquiry information submitted through “Contact Us”	LeaveHomeSafe servers in Government Private Cloud. All internet incoming traffic will be protected by HTTPS protocol.	Will be kept for 7 years or less when the data are no longer required.

Data involved	Security Measures applied	Data Removal
Taxi Registration Mark OCR	The OCR function is performed offline locally in the app and no internet connection is required for the OCR.	The image will not be stored in the system, including the mobile app and server.
Electronic COVID-19 Vaccination and Testing record	Encrypted using AES-256 and stored in local mobile phones. Local authentication relies on OS biometric authentication like face or fingerprint, providing a fallback like passcode or PIN when biometrics are not available	Can be manually removed by users at any time at their wish.
Motion Sensor data (Dynamic Auto-leave Function)	No storage	Immediately removed after the user activity recognition.
HCS Login Information (except password) (Under "Remember Login Information" function)	Encrypted using AES-256 and stored in local mobile phones. The identity document number is masked when it is retrieved from the "Remember Login Information" function and displayed.	Can be manually removed by users at any time at their wish
History of Uploaded Visit Records and Notification Records to HCS (for registered users of HCS)	The identify document numbers in upload history is encrypted using AES-256 and stored in local mobile phones. The identity document numbers are masked in display.	Automatically removed after 31 days.

Privacy Risk Analysis Findings and Privacy Impact Revealed

In determining risks associated with the System, we have utilized the following model for classifying risk:

Risk = Threat Likelihood x Magnitude of Impact

And the definitions are as follows:

Threat Likelihood

Likelihood	Definition
High	Expected to occur in most circumstances
Medium	Should occur occasionally
Low	Could occur at specific time or in exceptional circumstances

Magnitude of Impact

Impact	Definition
High	Most significant: major loss and seriously damaging the organization; severe, catastrophic, or serious long-term damage / disruption

Medium	Significant: medium loss which would be detrimental to the organization; serious short-term, or limited long-term damage / disruption
Low	Least significant: low loss which would cause little or no damage to the organization; limited and short-term damage / disruption

Risk rating is used to represent the overall effects of impact and the corresponding likelihood, which is defined as follows:

Risk Model Matrix

Risk		Likelihood		
		High	Medium	Low
Impact	High	**High**	**Medium**	**Medium**
	Medium	**Medium**	**Medium**	**Low**
	Low	**Low**	**Low**	**AOI**

Risk rating and indicative implementation schedule are given below:

Risk rating	Implication and recommendation
H (high)	Means critical impact and improvements should be done immediately
M (medium)	Means moderate impact and improvements should be done within a short time
L (low)	Means low impact and improvements should be done within a reasonable time
AOI (area of improvement)	Does not impose immediate threats but implementation of such measures will improve the environment. These enhancements should be implemented when resources are available.

Risk Assessment Results

There is NO privacy risk and issue identified during the detailed privacy impact analysis since appropriate safeguards have been implemented to protect any personal data stored on the System. As there are no recommended measures to be implemented, PCA exercise and report are not required.

Compliance / Monitoring Mechanisms

According to the PIA checklist collected, the compliance status is listed below:

High level analysis	Summary of audited items	Compliance status (Fully/Partially/Non-compliance)
Amount of personal information involved in project	Only necessary information is collected to support mobile app and related support system for exposure notification process. Only with their express consent, users may at their sole discretion upload their visit records and notification records from the LeaveHomeSafe mobile app to the Hong Kong Health Code System after successfully login to HCS with login information.	Fully
Sensitivity of personal information	Personal information collected: • person responsible for registration of venue QR code: name, telephone number, e-mail address, supporting document file (e.g. BR certificate, licence / registration certificate or documents for respective sectors and scheduled premises, such as restaurants, karaoke, vehicles, owners' corporations, schools, etc.) • app users: vaccination records and testing results (name, identity document number, download date, vaccination date, vaccine name, specimen, specimen collection date, testing platform, test result, test result/ report date) • confirmed / preliminary positive cases of COVID-19: name, telephone number, in-/out-records (venue, enter / leave time) • enquirer: name, telephone number, e-mail address	Fully

High level analysis	Summary of audited items	Compliance status (Fully/Partially/Non-compliance)
	• Login information of HCS, including Identity document type, issuing country/region and identity document number	
All practicable steps shall be taken to notify the data subjects of the purpose of data collection and the classes of persons to whom the data may be transferred, according to DPP1.	PICS has been reviewed and the purpose of data collection is shown to be clearly mentioned.	Fully
All practicable steps shall be taken to ensure personal data is accurate and is not kept longer than necessary to fulfil the purpose for which it was originally collected according to DDP 2.	The retention period of any personal data is defined: 31 days for the stored visit records and notification records in mobile phones; 7 years in LeaveHomeSafe system	Fully
Personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless the data user obtains from the data subject voluntary and explicit consent to use the data for a new purpose, according to DPP 3.	Data are used for a directly related purpose.	Fully
DPP 4 — Security of personal data } Data user needs to take all practicable steps to safeguard personal data from unauthorized or accidental access, processing, erasure, loss or use.	Data are protected in different states – at rest, in transit, in motion.	Fully
DPP 5 — Openness of Information } Data user must take all practicable steps to make known to the public its personal data policies and practices, types of personal data it holds and the main purposes for which it uses the data.	Mentioned in the updated PICS and PPS are reviewed. The visit records and notification records to be uploaded to the Hong Kong Health Code System will be subject to the collection, holding, processing or use of the data concerned by the Hong Kong Health Code System. Please read	Fully

High level analysis	Summary of audited items	Compliance status (Fully/Partially/Non-compliance)
	the Hong Kong Health Code System's Personal Information Collection Statement and Privacy Policy Statement.	
Data subject has the right to request access to his/ her own personal data, and request the correction of the personal data if it is inaccurate according to DPP 6.	Mentioned in PICS and reviewed.	Fully
Personal data breach handling	Comply with the security incident handling guidelines from OGCIO.	Fully

Recommendations

- ALL the security controls applied in the System are examined based on the requirements of DPPs stipulated by PDPO.
- It is suggested that PIA be conducted again for any system change after the System v3.0 is rolled out.

Conclusion

It is verified that the System is in total compliance with PDPO's requirements.