

Notes:

- *This report has been translated into Chinese. If there is any inconsistency between the English version and the Chinese version, the English version shall prevail.*
- *Consider the importance of information security, those not appropriate to be disclosed including the internal details of the system, are redacted.*

**Privacy Impact Assessment and Privacy Compliance
Audit
on the
Multi-functional Smart Lampposts Pilot Scheme
of the
Office of the Government Chief Information Officer**

Privacy Impact Assessment Report

Prepared By



Version: 1.1

Jul 2023

© The Government of the Hong Kong Special Administrative Region

The contents of this document remain the property of and may not be reproduced in whole or in part without the expressed permission of the Government of the HKSAR

Version History

Version	Date	Description	Author
1.0	10 Feb 2023	Completed Version	
1.1	10 Jul 2023	Minor updates and editing	

Distribution

Copy No.	Holder
1	Office of the Government Chief Information Officer (“OGCIO”)
2	

Table of Contents

1. DEFINITIONS AND CONVENTIONS.....	2
1.1. DEFINITION	2
1.2. CONVENTION	2
2. EXECUTIVE SUMMARY.....	3
2.1. PRIVACY ISSUE FINDINGS AND RECOMMENDATIONS SUMMARY	3
2.2. CONCLUSION.....	4
3. BACKGROUND.....	5
4. SCOPE AND OBJECTIVE.....	6
5. SUMMARY OF ASSESSMENT ACTIVITIES.....	7
6. WORK PLAN.....	8
7. ASSUMPTIONS AND LIMITATIONS.....	9
8. ASSESSMENT METHODOLOGY	10
8.1. WORK APPROACH.....	10
8.2. PRINCIPLES APPLIED	12
8.3. PRIVACY ISSUES CLASSIFICATION.....	13
9. PERSONAL DATA FLOW ANALYSIS	14
9.1. DATA TYPES AND DATA FLOW	14
9.2. DATA TYPE & DATA FLOW TABLE	15
10. PRIVACY ANALYSIS	17
10.1. PRIVACY FINDING SUMMARY	18
11. IDENTIFICATION OF THE PRIVACY RISKS	19
11.1. PRINCIPLE 1 -- PURPOSE AND MANNER OF COLLECTION OF PERSONAL DATA	19
11.2. PRINCIPLE 2 -- ACCURACY AND DURATION OF RETENTION OF PERSONAL DATA.....	20
11.3. PRINCIPLE 3 – USE OF PERSONAL DATA	20
11.4. PRINCIPLE 4 -- SECURITY OF PERSONAL DATA	20
11.5. PRINCIPLE 5 – INFORMATION TO BE GENERALLY AVAILABLE	21
11.6. PRINCIPLE 6 -- ACCESS TO PERSONAL DATA	22
11.7. ISO/IEC 27701:2019 – PRIVACY INFORMATION MANAGEMENT.....	23
12. OVERALL OPINION.....	28
13. APPENDIX I – LIST OF DOCUMENTATIONS.....	29
14. APPENDIX II – LIST OF DEVICES OF THE IT SUPPORT SYSTEM AND RELATED COMPONENTS.....	30
15. APPENDIX III – INTERVIEW SAMPLE QUESTIONS.....	31

1. Definitions and Conventions

1.1. Definition

Data subject	It is a living individual to whom personal data relates. (e.g. general public, citizen)
Data user	It means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the personal data. (e.g. clerical user, manager)
Data processor/operator	It is a person who processes personal data on behalf of another person. (e.g. IT operator, system administrator)
Personal data system	It is a system which is used by a data user and includes any document and equipment forming part of the system.

1.2. Convention

AOI	Area of Improvement
HKSAR	Hong Kong Special Administrative Region
PCA	Privacy Compliance Audit
PCPD	Privacy Commissioner for Personal Data
PD(P)O	Personal Data (Privacy) Ordinance (Cap 486)
PIA	Privacy Impact Assessment
IT Support System	IT Support System of the Multi-functional Smart Lampposts Pilot Scheme
PIMS	Privacy Information Management System
System	Multi-functional Smart Lampposts and Associated Devices
DPP	Data Privacy Principles

2. Executive Summary

The Privacy Impact Assessment (PIA) is to examine the compliance status of the IT Support System and associated devices of the Multi-functional Smart Lampposts Pilot Scheme regarding Personal Data (Privacy) Ordinance (Cap.486) (PD(P)O), ISO/IEC27701:2019 and other relevant Ordinances, prevailing guidelines and recommendations from the Office of the Privacy Commissioner for Personal Data, and make reference to prevailing industry and international practices.

2.1. Privacy Issue Findings and Recommendations Summary

In this assessment, the System is in compliance with privacy principles of PD(P)O and ISO/IEC27701:2019 with the limitations set out in Section 6 of this report.

Summary of Findings

Privacy Principles	Findings			Compliance Status
	Failed compliance	Partial compliance	Area of Improvement (AOI)	
PD(P)O				
1	0	0	0	Yes
2	0	0	0	Yes
3	0	0	0	Yes
4	0	0	0	Yes
5	0	0	0	Yes
6	0	0	0	Yes
ISO 27701:2019				
A.7.2	0	0	0	Yes
A.7.3	0	0	0	Yes
A.7.4	0	0	0	Yes
A.7.5	0	0	0	Yes

Description of the risk level

- High:** If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
- Medium:** If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
- Low:** If an observation is described as low risk, the system's designated approving authority must determine whether corrective actions are still required or decide to accept the risk.
- AOI:** Informational as an area of improvement only.

Description of privacy principles

PD(P)O

Principle 1 -- Purpose and manner of collection of personal data

Principle 2 -- Accuracy and retention of personal data

RESTRICTED

Principle 3 -- Use of personal data
Principle 4 -- Security of personal data
Principle 5 -- Information to be generally available
Principle 6 -- Access to personal data

ISO/IEC 27001:2019

A.7.2 – Conditional for collection and processing
A.7.3 – Obligations to PII principals
A.7.4 – Privacy by design and privacy by default
A.7.5 – PII Sharing, transfer and disclosure

2.2. Conclusion

After the assessment of the IT Support System, there is no outstanding privacy issue / observation after this PIA stage. There are some points observed.

- 1) No privacy information was collected from any individual
- 2) No privacy data stored in IT Support System
- 3) Security measures are in place to protect personal data.
- 4) Security policy and regulation, and privacy policy statement are defined and can be accessed on the website.

3. Background

The Multi-functional Smart Lampposts Pilot Scheme (“the Pilot Scheme”) is one of the key infrastructure projects for smart city development which will be implemented in four selected urban locations, namely, Central and Admiralty; Wan Chai; Yau Tsim Mong; and Kwun Tong / Kai Tak Development Area. Under the Pilot Scheme, some 400 smart lampposts with smart devices will be installed in phases, with a view to collecting real-time city data such as air quality and traffic flow, enhancing city management as well as supporting the development of digital infrastructure for the fifth generation (5G) mobile communications services. As of December 2022, more than seventy (70) smart lampposts have been put into operation in Kwun Tong, Kowloon City, Kai Tak Development Area and Yau Tsim Mong. Some 300 remaining smart lampposts will be completed in phases in 2023.

To provide IT infrastructural support to the Pilot Scheme, an IT Support System with features including a telecommunications network, a devices management platform and an application system for data collection and transmission was set up and launched in June 2019. The IT Support System provides integrated IT services to the smart devices in the smart lampposts covered by the Pilot Scheme and maintains the connectivity between the smart lampposts and the application systems of the user departments through telecommunications network, cloud services and application system functions; monitor the healthiness of smart devices and communications devices in the smart lampposts and ensure security for data transmission.

4. Scope and Objective

The main objectives of this work assignment are to conduct PIA on the Multi-functional Smart Lampposts Pilot Scheme:

- a. Identify the data privacy potential effect, actual effects, implication, issues and risks;
- b. Perform data processing cycle analysis;
- c. Perform privacy risk analysis;
- d. Analyze fully and systematically the personal information flows and processing cycle in the IT Support System and Related Components; and clearly indicate the possible and potential privacy impacts and risks that the personal information flows may have on privacy;
- e. Provide recommendations on how the identified potential and actual effects upon personal data privacy can be mitigated;
- f. Assess and ensure compliance with the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) and other relevant Ordinances, prevailing guidelines, code of practices (COPs) and recommendations from the Office of the Privacy Commissioner for Personal Data;
- g. Provide recommendations on how to avoid or mitigate issues and risks;
- h. Recommend alternative or less privacy-intrusive practice with details in handling personal data to minimize or eradicate any identified privacy impacts so as to fully comply with the compliance level requirements as specified in Clause 3.1 (f) above by making reference to prevailing industry and international practices (particularly ISO 27701); and
- i. Conduct the Privacy Compliance Audit with the objective of reassessing whether the recommendations of the Privacy Impact Assessment have been adequately addressed; and
- j. Report and document the findings, recommendations and privacy protective measures in addressing the privacy risks.

RESTRICTED

5. Summary of Assessment Activities

Major Task	Detailed Task	Completion Data	Resources
Documents Review	Documentation Review	28 Oct 2022	
PIA Questionnaire Checklist	Questionnaire Checklist Review	28 Oct 2022	
Interview Discussions /	Interviews & discussions with IT support system team for smart lamppost of OGCIO by phone conversation	Oct 2022	
Privacy Impact Analysis	Personal Data Flow Analysis, Personal Data Privacy Analysis, Draft Mitigation Recommendation	3 Nov 2022	
Compilation of Report	Privacy Impact Assessment Report delivery	10 Feb 2023	

6. Work Plan

	Stage 2: Privacy Impact Assessment on System Analysis & Design of the IT Support System			
2.1	Conduct PIA	Questionnaire Checklist review		28 Oct 2022
		Interview on Zoom		
		Privacy Risk Analysis		
2.2	Compile PIA Report with Recommendations and conduct presentation	- PIA Report on SA&D with Recommendations and Follow-up Plan - Presentation Materials		04 Nov 2022
	Stage 3: Privacy Compliance Audit on the System Production of the IT Support System			
3.1	Conduct PCA			02 Dec 2022
3.2	Compile audit report and conduct presentation	- PCA Report and Follow-up Plan - Presentation Materials		09 Dec 2022
	Stage 4: Project Closure			
4.1	Finalize Executive Summary and Presentation	- Final Executive Summary - Presentation Materials		23 Dec 2022

7. Assumptions and Limitations

The current privacy impact assessment is based on the available documents, questionnaire checklist, communication networks, hardware and software in scope.

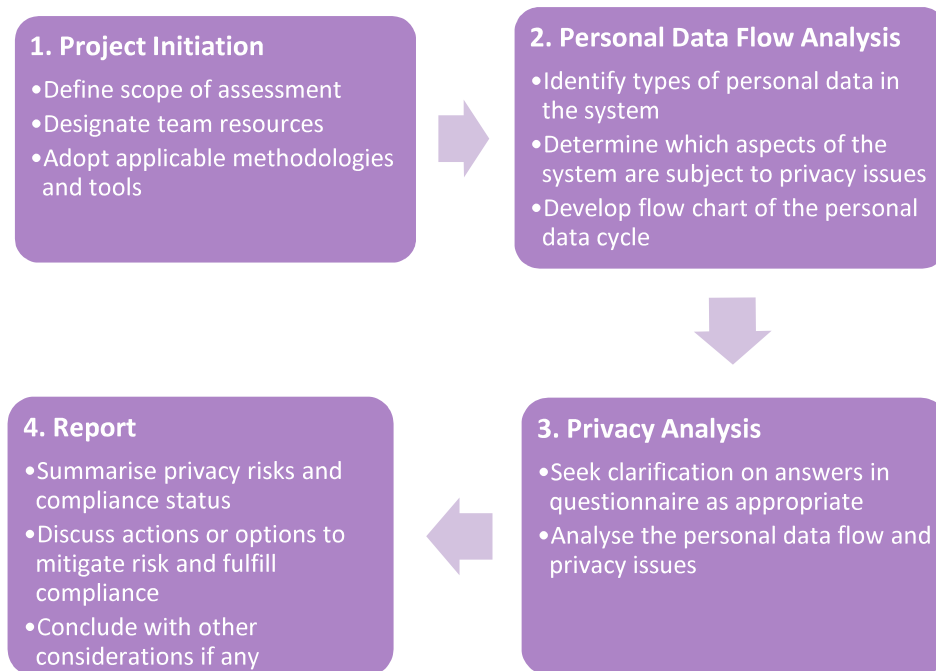
8. Assessment Methodology

8.1. Work Approach

The PIA process has four core phases:

- a. Project Initiation
- b. Personal Data Flow Analysis
- c. Privacy Analysis
- d. Report

The following chart summarises the key activities of the four phases of the PIA process



Phase 1: Project Initiation

At the initiation stage, the PIA consultant performed the following key activities:

- a. Defining the scope and the schedule of the PIA.
- b. Designating team resources for the provision of service.
- c. Clarifying the roles and responsibilities of the system owners, data users and other stakeholders.
- d. Verifying applicability of the local legislative and policy authorities for the system.
- e. Selecting the applicable methodology and tools to be used.

Phase 2: Personal Data Flow Analysis

This activity involves a description and analysis of the business processes, system architecture, and data flows. The purpose of this step is to depict the personal data flows.

Below are the key activities of the Personal Data Flow Analysis phase:

- a. Identifying elements, types, volume or clusters of personal data being collected, used, disclosed and retained.
- b. Analysing the flow of personal data through business process diagrams.
- c. Determining which aspects of the system are subject to privacy issues.
- d. Developing a data flow chart of the handling of personal data.

Phase 3: Privacy Analysis

The privacy analysis examines the flow of personal data in the context of applicable privacy policies and legislation.

Below are the key activities of the Privacy Analysis phase:

- a. Reviewing the relevant policies, procedural manuals, specifications and materials in the handling of personal data.
- b. Analysing the flow of personal data and potential privacy issues against the Data Protection Principles issued by the PCPD, the Security Regulations by the Security Bureau as well as any other relevant privacy policies and circulars in OGCIO.
- c. Identified privacy impacts so as to fully comply with the compliance level requirements as specified in reference to ISO27701:2019 prevailing industry and international practices
- d. Producing an initial draft report on preliminary finding(s).

The PIA consultant has conducted the above steps with the assistance provided by OGCIO staff so as to assess the privacy issues, impacts and implications of the system.

Phase 4: Report

Based on the outputs from the previous steps, this is the final and most critical component of the PIA process. This is a documented evaluation of the privacy issues and the associated implications of those issues along with proposals on remedies or mitigation strategies.

RESTRICTED

Below are the key activities of the Report phase:

- a. Summarising the PIA findings and recommending safeguard to mitigate the privacy risk and fulfil the compliance requirement.
- b. Discussing each privacy issue item with OGCIO, relevant B/Ds and parties and address queries, if any.
- c. Compiling this report.

8.2. Principles Applied

For this work assignment, [REDACTED] made reference including but not limited to the Personal Data (Privacy) Ordinance and related guidelines refer to the Personal Data (Privacy) Ordinance (Cap. 486) and other relevant Ordinances, prevailing guidelines and recommendations from the Office of the Privacy Commissioner for Personal Data.

The six principles of PD(P)O were used in accessing and examining the system. These principles are:

Principle 1 -- Purpose and manner of collection of personal data

This provides for the lawful and fair collection of personal data and the requirement for the data subjects to be notified of the purpose and the classes of persons to whom the data may be transferred.

Principle 2 -- Accuracy and retention of personal data

This provides that personal data should be accurate, up-to-date and kept no longer than necessary to fulfil the purposes for which the data is used.

Principle 3 -- Use of personal data

This provides that unless the data subject gives consent, personal data should be used for the purposes for which they were collected or a directly related purpose.

Principle 4 -- Security of personal data

This requires appropriate security measures to be applied to safeguard personal data (including data in a form in which access to or processing of the data is not practicable).

Principle 5 -- Information to be generally available

This requires data users to take practicable steps to make personal data policies and practices known to the public/data subjects regarding the types of personal data they hold and how the data is used.

Principle 6 -- Access to personal data

This provides for data subjects being given access to their personal data and right to make correction.

8.3. Privacy Issues Classification

There will be two compliance status for each finding analysed by the PIA consultant(s). They are partial non-compliant and failed non-compliant. The failed non-compliant privacy issues are concluded by the PIA consultant(s) when the fact and evidence of the system is not compliant to the PD(P)O. Such violation will deprive the personal data subject of his/her privacy right and/or cause damage to the reputation of the OGCIO. The partial non-compliant status will be concluded when the PIA consultant finds when a) the fact and evidence of the system is not fully compliant to the PD(P)O but there are some safeguards implemented to certain extent, or b) there are some but not sufficient fact and evidence to conclude the violation against the PD(P)O.

In addition to these two classifications, finding will be classified as Area of Improvement (AOI) aka Observation. The findings which do not violate directly the data protection principles can be taken with recommended safeguard to further improve the protection of personal data.

During the analysis of identified privacy items, a consistent privacy modelling approach based on qualitative analysis is used to portray the items based on factors such as the kind of personal identifiers in question, compliance with the PD(P)O or Data Protection Principles as referred to under the PD(P)O on the confidentiality and integrity against likelihood and impact severity of the personal data.

			Impact Severity		
			High	Medium	Low
			3	2	1
Likelihood	High	3	9	6	3
	Medium	2	6	4	2
	Low	1	3	2	1

High
Medium
Low

The score of a privacy item is calculated by multiplying its likelihood and impact severity scores. A higher score reflects a higher priority issue, which should be addressed sooner. Each of the items is then classified as high, medium and low based on the following classification scheme:

- ♦ High Priority: score ≥ 6
- ♦ Medium Priority: $3 \leq \text{score} < 6$
- ♦ Low Priority = score < 3

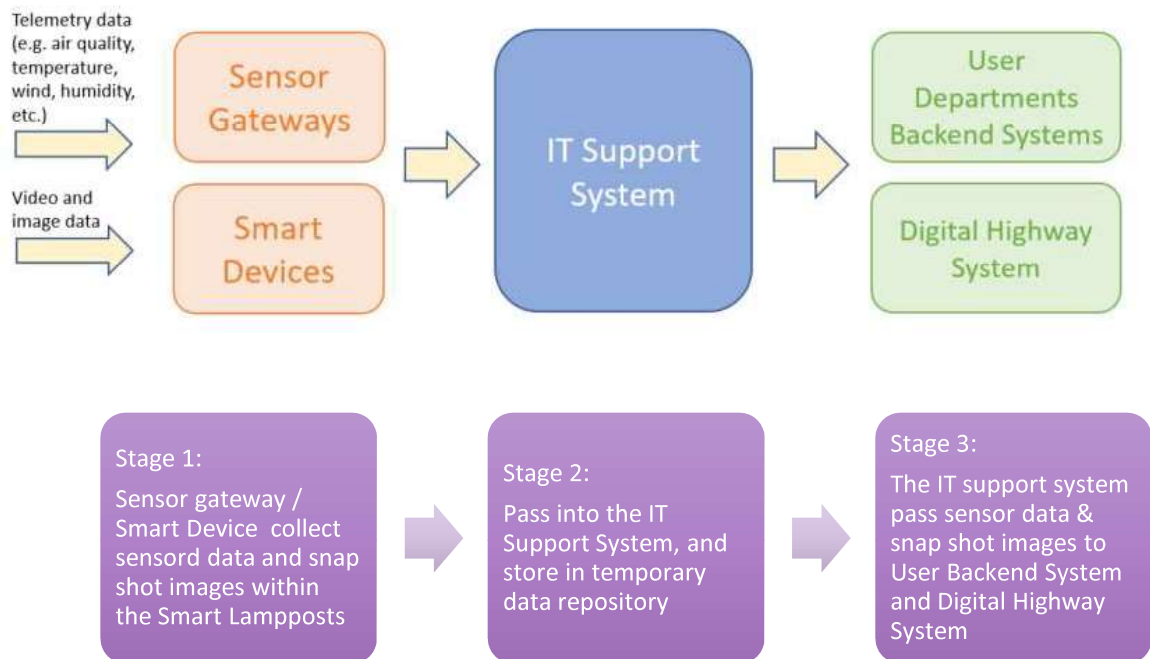
The high priority items require immediate attention and prudent rectification actions. The rectification actions for medium priority items can be prioritised after the high priority items depending on the resources availability. Attention for low priority items can be put at last. A longer duration will be allowed to rectify the low priority items. All in all, these items of high/medium/low priority are treated as non-compliance item to the PD(P)O, which are required to take actions promptly.

Corresponding recommendations will be provided for consideration.

9. Personal Data Flow Analysis


9.1. Data Types and Data Flow

Below present the stages in the processing flow of video and image data in the IT Support System.





9.2. Data Type & Data Flow Table

The following table summarise the information on data capture, data processes, data stores, data transfer, and data disposal of each device for assessment.

Smart Device / Sensor Gateway	Data Item	Personal Data (Y/N)	Data Capture	Data Store at Smart Lamppost	Data Transfer to IT Support System	Data Output To Digital Highways	Data Transfer (Data User)	Data Disposal (Data User)
Weather Stations	Collect meteorological data at district level including temperature and relative humidity, wind speed and direction and rainfall amount	N	Capture through Sensors	No data storage	Stored in the temporary data repository	Y	To HKO	Keep 7 days, and delete automatically
Gamma Sensor	Gamma radiation level	N	Capture through Sensor	No data storage	Stored in the temporary data repository	Y	To HKO	Keep 7 days, and delete automatically
Air Quality Sensor	Collect air quality data including concentration of nitrogen monoxide, nitrogen dioxide and PM 2.5 at district level	N	Capture through Sensor	No data storage	Stored in the temporary data repository	Y	To EPD	Keep 7 days, and delete automatically
Thermal Detector	Thermal images on moving vehicles, bicycles and pedestrians. 	N	Capture through Sensor	Local Storage	No data pass through IT Support System	Y	To TD	Deleted automatically
Bluetooth Beacon	Transmit 2.4 GHz Bluetooth signals for providing accurate position information, only send out Bluetooth signals	N	NA	No data storage	No data pass through IT Support System	Y	To Data user	Deleted automatically

RESTRICTED

Geo-QR Code Tag	Provide pedestrians with accurate position information for location-based applications Provide a platform for pedestrians to search nearby public facilities, such as toilet, clinic, post office, MTR entrance, etc.		N	NA	NA	No data collection	Y	To data user	NA
RFID Tag	RFID Tag		N	NA	NA	No data collection	Y	To data user	NA
NFC Tag	NFC technology provides more secure and reliable position data to users for applications		N	NA	NA	No data collection	Y	To data user	NA
LiDAR	LiDAR images of different types of vehicles in the traffic and their speed.		N	Capture through Sensor	Local Storage	No data pass through IT Support System	Y	To TD	Delete automatically
Network Equipment 1) LTE Router 2) Fibre Switch 3) PoE Switch	Network Equipment handling sensor data that receive and transmit to IT Support System.		N	Capture through Sensor	NA	Yes	NA	NA	NA

10. Privacy Analysis

PIA consultant performed the following procedures during the assessment:

Document Review¹

A list of system documents was reviewed to understand and analyse the design of the IT Support System.

Interview²

The consultant then mutually understood the IT Support System in the aspects of six DPPs with the stakeholders in a briefing and Q&A session. Afterwards, the representatives of B/Ds replied the questions along with documents such as their relevant system procedures and manuals. The consultants studied the replies and the documents, meanwhile queries were clarified with the representative individually.

Personal Data Collection Process

Collection - After review the systems include of devices, documents, and the application and infrastructure platform, the System will not collect personal data on its own.

The IoT sensors are collecting environmental data from the public areas near the smart lampposts such as the temperature, relative humidity, average wind speed, average wind direction, NO (ppb), NO₂ (ppb), PM_{2.5}, Gamma ray data.

LiDAR images of different types of vehicles in the traffic and their speed. Thermal images on moving vehicles, bicycles and pedestrians. Both images are personal identities can't be determined.

Use, Disclosure, and Retention of Personal Data

Use - After review the systems include of devices, documents, and the application and infrastructure platform, the System will not use personal data on its own.

Disclosure - There is no privacy information collected from any individual, no personal data in the system will be disclosed.

Retention - There is no privacy information collected from any individual, no personal data of any kind left in the system.

IT Support System only stores meteorological data and air quality data for 7 days, and the data is deleted automatically. The Thermal images and LiDAR images are deleted automatically in the smart lampposts.

The IT Support System receives the sensor data, temporary stored it and forward these data to user department using Digital Highway of OGCIO through the Internet Bandwidth Service (IBS) provided by OGCIO. The Digital Highway will share these data to departmental backend systems (e.g. HKO, EPD) at departmental data centre through the GNET network connection.

¹ List of documentations reviewed is at **Appendix I**.

² List of questions discussed is at **Appendix II**.

RESTRICTED

Security Measure of Personal Data

The System conforms to the Government's Security Regulations, Baseline IT Security Policy [S17] and IT Security Guidelines [G3] for handling personal data (classified as RESTRICTED at least). Security Risk Assessment and Audit ("SRAA") will be conducted periodically on the security safeguards of the System for preventing unauthorised or accidental access to, processing, erasure, loss or use of the data. Each B/D has its own Privacy Policy and Personal Information Collection Statement for the components it was involved. There are reviews on the types of data collected. If there is personal data collected, there will be privacy protection measures implemented. Currently, there is no privacy information collected from any individual.

The data was transmitted and stored with contemporary encryption algorithm. Access control was considered to prevent the recording from falling into the wrong hands at the lamppost.

IT Support System in the public cloud through the Cloud Broker Service provided by the services provider. The VPN Gateway option on the public cloud can be enabled to provide the secure network tunnel for data collection by the IT Support System.

10.1. Privacy Finding Summary

The following table summarises all the privacy issues identified and reviewed during the PIA exercise as refer to Clause 3 (d) of this document:

Privacy Principles	Findings			Compliance Status
	Failed compliance	Partial compliance	Area of Improvement (AOI)	
PD(P)O				
1	0	0	0	Yes
2	0	0	0	Yes
3	0	0	0	Yes
4	0	0	0	Yes
5	0	0	0	Yes
6	0	0	0	Yes
ISO 27701:2019				
A.7.2	0	0	0	Yes
A.7.3	0	0	0	Yes
A.7.4	0	0	0	Yes
A.7.5	0	0	0	Yes

11. Identification of the Privacy Risks

For the benefit of understanding of the privacy issues identified in this report and their levels of privacy risk priority, the findings are grouped under the six Data Protection Principles.

11.1. Principle 1 – Purpose and manner of collection of personal data

No.	Items	Compliance Status (Y/N/NA)	Remarks
1	Personal data are collected for a lawful purpose.	NA	No privacy information collected from any individual
2	Personal data are collected directly related to a function or activity of the data user who is to use the data.	NA	No privacy information collected from any individual
3	Personal data collected are adequate but not excessive in relation to the purpose.	NA	No privacy information collected from any individual
4	Personal data are collected by lawful means.	NA	No privacy information collected from any individual
5	Personal data are collected by means which are fair in the circumstances of the case.	NA	No privacy information collected from any individual
6	Data subjects are explicitly or implicitly informed on or before collecting the data of whether it is obligatory or voluntary for him to supply the data. Where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data.	NA	No privacy information collected from any individual
7	Data subjects are explicitly informed on or before collecting the data of the purpose (in general or specific terms) for which the data are to be used.	NA	No privacy information collected from any individual
8	Data subjects are explicitly informed on or before collecting the data of the classes of persons to whom the data may be transferred.	NA	No privacy information collected from any individual
9	Data subjects are explicitly informed on or before first use of the data for the purpose for which they were collected of his rights to request access to and to request the correction of the data and the name and address of the individual to whom any such request may be made.	NA	No privacy information collected from any individual

No issue of non-compliance is identified under this principle.

RESTRICTED

11.2. Principle 2 – Accuracy and duration of retention of personal data

No.	Items	Compliance Status (Y/N/NA)	Remarks
1	Personal data are accurate having regard to the purpose (including any directly related purpose) for which the personal data are or are to be used.	NA	No privacy information collected from any individual
2	When there are reasonable grounds for believing that personal data are inaccurate, the personal data will not be used for the purpose.	NA	No privacy information collected from any individual
3	Personal data will not be kept longer than is necessary for the fulfilment of the purpose.	NA	No privacy information collected from any individual
4	Data users (including third party) will be informed when the collected personal data is found inaccurate.	NA	No privacy information collected from any individual

No issue of non-compliance is identified under this principle.

11.3. Principle 3 – Use of personal data

No.	Items	Compliance Status (Y/N/NA)	Remarks
1	Personal data will be used for the purpose for which the data were to be used at the time of the collection of the data.	NA	No privacy information collected from any individual
2	Personal data will be used for the purpose directly related to the purpose mentioned above.	NA	No privacy information collected from any individual

No issue of non-compliance is identified under this principle.

11.4. Principle 4 – Security of personal data

No.	Items	Compliance Status (Y/N/NA)	Remarks
1	Personal data are protected against unauthorized or accidental access physically.	NA	No privacy information collected from any individual The data was transmitted and stored with

RESTRICTED

			contemporary encryption algorithm. Access control was considered to prevent the recording from falling into the wrong hands at the lamppost.
2	Personal data are stored in equipment with practicable security measures.	NA	No privacy information collected from any individual The data was transmitted and stored with contemporary encryption algorithm. Access control was considered to prevent the recording from falling into the wrong hands at the lamppost.
3	Measures will be in place to ensure the integrity of the personal data.	NA	No privacy information collected from any individual. Access Control, Data Encryption to ensure the data integrity.
4	Measures will be in place to ensure the secure transmission of the data.	Y	VPN established to provide the secure network tunnel for data collection by the IT Support System.

No issue of non-compliance is identified under this principle.

11.5. Principle 5 – Information to be generally available

No.	Items	Compliance Status (Y/N/NA)	Remarks
1	Data users will be informed of the main purposes of the usage of the personal data before using the personal data.	NA	No privacy information collected from any

RESTRICTED

			individual
2	Data users will be briefed the security and usage awareness in handling personal data before using the personal data.	NA	The importance of privacy protection related to the system has been stated in the “Report of the Technical Advisory Ad Hoc Committee on Multi-functional Smart Lampposts”.

No issue of non-compliance is identified under this principle.

11.6. Principle 6 – Access to personal data

No.	Items	Compliance Status (Y/N/NA)	Remarks
1	Data subjects will be able to verify with data user about the type of their personal data that being stored, used and distributed.	NA	No privacy information collected from any individual
2	Data subjects will be able to request the correction of personal data.	NA	No privacy information collected from any individual
3	Data subjects will be given reasons if their request to access their personal data that being stored is refused.	NA	No privacy information collected from any individual

No issue of non-compliance is identified under this principle.

11.7. ISO/IEC 27701:2019 – Privacy Information Management

ISO 27701:2019 details this guidance for the establishment, implementation, maintenance and improvement of a Privacy Information Management System (PIMS). The standard is based on the requirements, control objectives and controls of the ISO 27701:2019 standard, and includes a suite of privacy requirements, controls and control objectives.

The table contains the categories having a control objective, following with the proposed controls. The implementation guidance is included in the ISO 27701 standard.

Control No.	PIMS specific guidance for Data Controllers		Compliance
	Control	Description	
A.7.2	To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.		Yes
A.7.2.1	Identify and document purpose	The organization shall identify and document the specific purposes for which the <i>personal data</i> will be processed.	Yes
A.7.2.2	Identify lawful basis	The organization shall determine, document and comply with the relevant lawful basis for the processing of <i>personal data</i> for the identified purposes.	Yes
A.7.2.3	Determine when and how consent is to be obtained	The organization shall determine and document a process by which it can demonstrate if, when and how consent for the processing of <i>personal data</i> was obtained from <i>data subjects</i> .	Yes
A.7.2.4	Obtain and record consent	The organization shall obtain and record consent from <i>data subjects</i> according to the documented processes.	Yes
A.7.2.5	Privacy impact assessment	The organization shall assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of <i>personal data</i> or changes to existing processing of <i>personal data</i> is planned.	Yes
A.7.2.6	Contracts with <i>personal data</i> processors	The organization shall have a written contract with any <i>data</i> processor that it uses, and shall ensure that their contracts with <i>data</i> processors address and implements all the required information contained within ISO 27701 Annex B	Yes
A.7.2.7	Joint <i>data</i> controller	The organization shall determine respective roles and responsibilities for the processing of <i>personal data</i> (including <i>personal data</i> protection and security requirements) with any joint <i>data</i> controller.	Yes

RESTRICTED

Control No.	PIMS specific guidance for Data Controllers		Compliance
	Control	Description	
A.7.2.8	Records related to processing <i>personal data</i>	The organization shall determine and securely maintain the necessary records in support of its obligations for the processing of <i>personal data</i> .	Yes
A.7.3	To ensure that <i>data subjects</i> are provided with appropriate information about the processing of their <i>personal data</i> and to meet any other applicable obligations to <i>data subjects</i> related to the processing of their <i>personal data</i> .		Yes
A.7.3.1	Determining and fulfilling obligations to <i>data subjects</i>	The organization shall determine and document their legal, regulatory and business obligations to <i>data subjects</i> related to the processing of their <i>personal data</i> and provide the means to meet these obligations.	Yes
A.7.3.2	Determining information for <i>data subjects</i>	The organization shall determine and document the information to be provided to <i>data subjects</i> regarding the processing of their <i>personal data</i> and the timing of such a provision.	Yes
A.7.3.3	Providing information to <i>data subjects</i>	The organization shall provide <i>data subjects</i> with clear and easily accessible information identifying the <i>data controller</i> and describing the processing of their <i>personal data</i> .	Yes
A.7.3.4	Providing mechanism to modify or withdraw consent	The organization shall provide a mechanism for <i>data subjects</i> to modify or withdraw their consent.	Yes
A.7.3.5	Providing mechanism to object to <i>personal data</i> processing	The organization shall provide a mechanism for data subject to object to the processing of their <i>personal data</i> .	Yes
A.7.3.6	Access, correction and/or erasure	The organization shall implement policies, procedures and/or mechanisms to meet their obligations to data subjects to access, correct and/or erase their personal data.	Yes

RESTRICTED

Control No.	PIMS specific guidance for Data Controllers		Compliance
	Control	Description	
A.7.3.7	<i>Data controllers' obligations to inform third parties</i>	The organization shall inform third parties with whom <i>personal data</i> has been shared of any modification, withdrawal or objections pertaining to the shared <i>personal data</i> , and implement appropriate policies, procedures and/or mechanisms to do so.	Yes
A.7.3.8	Providing copy of <i>personal data</i> processed	The organization shall be able to provide a copy of the <i>personal data</i> that is processed when requested by the <i>data subject</i> .	Yes
A.7.3.9	Handling requests	The organization shall define and document policies and procedures for handling and responding to legitimate requests from <i>data subjects</i> .	Yes
A.7.3.10	Automated decision making	The organization shall identify and address obligations, including legal obligations, to the <i>data subjects</i> resulting from decisions made by the organization which are related to the <i>data subject</i> based solely on automated processing of <i>personal data</i> .	Yes
A.7.4	To ensure that processes and systems are designed such that the collection and processing (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.		Yes
A.7.4.1	Limit collection	The organization shall limit the collection of <i>personal data</i> to the minimum that is relevant, proportional and necessary for the identified purposes.	Yes
A.7.4.2	Limit processing	The organization shall limit the processing of <i>personal data</i> to that which is adequate, relevant and necessary for the identified purposes.	Yes
A.7.4.3	Accuracy and quality	The organization shall ensure and document that <i>personal data</i> is as accurate, complete and up-to-date as is necessary for the purposes for which it is processed, throughout the life-cycle of the <i>personal data</i> .	Yes

RESTRICTED

Control No.	PIMS specific guidance for Data Controllers		Compliance
	Control	Description	
A.7.4.4	<i>Personal data</i> minimization objectives	The organization shall ensure and document that <i>personal data</i> is as accurate, complete and up-to-date as is necessary for the purposes for which it is processed, throughout the life-cycle of the <i>personal data</i> .	Yes
A.7.4.5	<i>Personal data</i> de-identification and deletion at the end of processing	The organization shall define and document data minimization objectives and what mechanisms (such as de-identification) are used to meet those objectives.	Yes
A.7.4.6	Temporary files	The organization shall either delete <i>personal data</i> or render it in a form which does not permit identification or re-identification of <i>data subjects</i> , as soon as the original <i>personal data</i> is no longer necessary for the identified purpose(s).	Yes
A.7.4.7	Retention	The organization shall not retain <i>personal data</i> for longer than is necessary for the purposes for which the <i>personal data</i> is processed.	Yes
A.7.4.8	Disposal	The organization shall have documented policies, procedures and/or mechanisms for the disposal of <i>personal data</i> .	Yes
A.7.4.9	<i>Personal data</i> transmission controls	The organization shall subject <i>personal data</i> transmitted (e.g. sent to another organization) over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.	Yes
A.7.5	To determine whether and document when <i>personal data</i> is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.		Yes
A.7.5.1	Identify basis for <i>personal data</i> transfer between jurisdictions.	The organization shall identify and document the relevant basis for transfers of <i>personal data</i> between jurisdictions.	Yes

RESTRICTED

Control No.	PIMS specific guidance for Data Controllers		Compliance
	Control	Description	
A.7.5.2	Countries and international organizations to which <i>personal data</i> can be transferred.	The organization shall specify and document the countries and international organizations to which <i>personal data</i> can possibly be transferred.	Yes
A.7.5.3	Records of transfer of <i>personal data</i>	The organization shall record transfers of <i>personal data</i> to or from third parties and ensure cooperation with those parties to support future requests related to obligations to the <i>data subjects</i> .	Yes
A.7.5.4	Records of <i>personal data</i> disclosure to third parties.	The organization shall record disclosures of <i>personal data</i> to third parties, including what <i>personal data</i> has been disclosed, to whom and at what time.	Yes

12. Overall Opinion

After the assessment of the IT Support System, there is no outstanding privacy issue / observation after this PIA stage. There are some points observed.

- 1) No privacy information was collected from any individual
- 2) No privacy data stored in IT Support System
- 3) Security measures are in place to protect personal data.
- 4) Security policy and regulation, and privacy policy statement are defined and can be accessed on the website.

13. Appendix I – List of Documentations

- T260+T340 System And Security Incident Handling Procedure v1.0.docx
- T240 User Operation Manual v1.1.docx
- T190 Application Operation Manual v1.1.docx
- T110 Physical Design Report v1.1.docx
- T100 Systems Analysis and Design Report v1.1.docx
- Privacy Policy Statement (Smart Lampposts).docx
- OGCIO IT Security Guideline [G3]
- OGCIO Baseline IT Security Policy [S17]
- ISO/IEC 27701:2019, First edition, August 2019
- Cap.486 Personal Data (Privacy) Ordinance of Hong Kong
- FLIR ThermiCami_IT_0013_EN.PDF
- i.Thermal-ThermiCAM2 390.PDF
- OS1 LiDAR Sensor Datasheet (64 Channel).pdf

14. Appendix II – List of devices of the IT Support System and related components

- Weather stations
- Gamma sensor
- Air quality sensor
- Thermal detector
- Bluetooth beacon
- Geo-QR Code Tag
- RFID tag
- NFC tag
- LiDAR
- Network Equipment, such as LTE Router, Fibre Switch and PoE Switch

15. Appendix III – Interview Sample Questions

No.	Sample Questions for conducting the Privacy Impact Assessment (PIA)
DPP1: Purpose and manner of collection of personal data	
1	What kinds of privacy information are involved?
2	What is the purpose of collecting the privacy information?
3	Who is accessible to the data? What is the purpose for providing data and how is it used?
4	Is the data subject explicitly informed the purpose for which the data used?
5	Is the data subject explicitly or implicitly informed, on or before collecting the data? When and how will that consent be obtained?
6	Is the data subject informed whether it is obligatory or voluntary for him to supply the data?
7	If obligatory, is the data subject informed the consequences if he/she fails to supply the data?
8	Is the data subject explicitly informed the classes of persons to whom the data may be transferred?
9	How is an assessment made to the adequacy and relevance (i.e. no more than the minimum required) of personal data for the purpose for which it is collected?
10	Is the Personal Information Collection Statement available and accessible to the data subject?
DPP2: Accuracy and duration of retention of personal data	
11	How personal data is checked for accuracy?
12	Are there procedures to determine when and how often personal data requires updating?
13	Are there procedures to monitor the factual relevance and timeliness of free text options or other comments about individuals?
14	What are the criteria for determining retention periods of personal data? And, how often are these criteria to be reviewed?
15	How do you and/or your staff remove the personal data from the system whenever the data is no longer usable?

RESTRICTED

No.	Sample Questions for conducting the Privacy Impact Assessment (PIA)
DPP3: Use of personal data	
16	Does the use (which term includes disclosure and transfer) of personal data continually fall within the original purpose of collection or its directly related purpose?
17	Does the project involve the use of existing personal data for new purpose without the consent of data subject?
18	Are the personal data transferred to Overseas? (e.g. via cloud computing)
DPP4: Security of personal data	
19	Is there a Data Security Policy or the like?
20	How your staff is made aware of Data Security Policy and instructed to make disclosures upon request?
21	What are the procedures for monitoring compliance with the Data Security Policy? Please list out the privacy protection measures implemented in the system.
22	What reasonable steps did you and/or your staff take to ensure that the data processor complies with data protection requirements? Please list out the privacy protection limitation noted in the system, whichever applicable.
23	Please describe security measures that are in place to prevent any unauthorised or unlawful processing of: a. Data held in an automated format (e.g. password controlled access to PCs) b. Data held in a manual record (e.g. locked filing cabinets)
24	Please describe risk management procedures to recover data (both automated and manual) which may be damaged/lost through human error, computer virus, network failure, theft, fire, flood or other disaster.
25	Please describe the procedures in place to detect and report breaches of data security (remote, physical or logical).
DPP5: Information to be generally available	
26	Are there any privacy policies and practices in place and made generally available and easily accessible for the below elements? - Kind of personal data in the system - Purposes for which personal data held - Proper mechanism for retention, erasure or destruction of personal data records - Data security measures in place
27	Is the Privacy Policy Statement effectively communicated to all the persons affected?

RESTRICTED

No.	Sample Questions for conducting the Privacy Impact Assessment (PIA)
DPP6: Access to personal data	
28	Is the data subject explicitly informed his rights to request access to and to request the correction of the data?
29	Is the data subject explicitly informed the contact name and address of the individual to whom any request may be made?
30	Are procedures in place to provide access to records (including any appropriate 'accessible' records, online or offline) request by the data subject?

<End of this document>