Personal Data Privacy Impact Assessment (PIA) Form

This document helps users access the impact of personal data privacy in their projects or systems. To learn more about Privacy Impact Assessment, please refer to the Privacy Impact Assessments (PIA) Leaflet from Office of the Privacy Commissioner for Personal Data (PCPD).

Please fill in the answers for the questions below. Save the document and send it back to ITSO at seccomp@ust.hk . If the handling of personal data in your application is changed after the form is submitted, you are requested to revise the form to reflect the latest changes and send it to us again.

Part 1: Background Information of the Proposed Project or System

Name of the Project or System:	
Department:	
Owner of the Project or System (Name & Email):	Name: Email:
Expected date of implementation:	
Description of the purpose of the project:	
Description of the benefits to the data subjects involved:	
Description of the risks to the data subjects involved	

Part 2: Data Processing Cycle Analysis

Description of the flow of handling personal data.	
Types of personal data to be collected (e.g. name, date of birth, Identity Card number, address, telephone number, etc.)	
Estimated number of data subjects from whom data is collected.	
Will any data processor(s) be involved? • If **yes**, please elaborate the measures to safeguard the data entrusted to the data processors. • If **no** measures are to be taken, please elaborate on the justification.	
Will there be any transfer of personal data to a country outside of Hong Kong? • If **yes**, please specify the destination(s) and the purpose(s) of transfer.	

Part 3: Privacy Risks Analysis

Areas	**PIA Questions**	**Answers**
Data Protection Principle (DPP) 1 – Data Collection Principle • Personal data must be collected in a lawful and fair way, for a purpose directly related to a function or an activity of the data user. • All practicable steps shall be taken to notify the data	Will the data subjects be informed of the purpose of collected their personal data? • If **yes**, please elaborate how. • If **no**, please provide justifications.	
	Please justify, item by item, why the collection of the personal data stated in Part 2 above is necessary	

Areas	PIA Questions	Answers
subjects of the purpose of the data collection and the classes of persons to whom the data may be transferred. • Data collected should be necessary but not excessive.	If Hong Kong identity card number/passport number will be collected, please elaborate whether the collection is in compliance with the PCPD's Code of Practice on the Identity Card Number and other Personal Identifiers.	
	If biometric data (e.g., fingerprint) is collected, please elaborate whether the collection is in compliance with the PCPD's Guidance Note on Collection and Use of Biometric Data.	
	Will the data subjects be informed, on or before the collection of the personal data, of whether the supply of the personal data is voluntary of obligatory? • If **no**, please provide justifications.	
	Where it is obligatory for data subjects to supply the personal data, will the data subjects be informed of the consequence of not providing the personal data? • If **yes**, please elaborate. • If **no**, please provide justifications	
	Will the data subject be informed of whether the personal data collected will be transferred or disclosed to any third parties? • If **yes**, please provide details of such third party. • If **no**, please provide justifications.	

Areas	PIA Questions	Answers
	If the personal data is to be transferred to any third party or data processor, will the data subjects be informed of the classes of persons to whom their personal data may be transferred or disclosed? • If **yes**, please provide details of the classes of person. • If **no**, please provide justification.	
DPP2 – Data Accuracy and Retention Principle • 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.	Will there be any measures in place to ensure accuracy of the personal data? • If **yes**, please elaborate • If **no**, please provide justifications.	
	Please specify the retention period of the personal data and justify it.	
	Will there be any measures in place to ensure that personal data is not kept longer than necessary to fulfil the purpose of using the data? • If **yes**, what are the measures; and how the data will be destroyed? • If **no**, please provide justifications.	
DPP3 – Data Use Principle • Personal data must be used for the purpose for which the data is collected or for a directly related purpose,	Will personal data be used only for the original purpose stated in the PICS? • If **no**, what are the other purposes?	

Areas	PIA Questions	Answers

unless the data user obtains from the data subject voluntary and explicit consent to use the data for a new purpose.	Where the personal data will be used for a new purpose:
	• Has explicit consent been obtained from the data subjects?
	  ○ If **yes**, please explain how.
	  ○ If **no**, please provide justification
	• What are the possible harms to the data subjects caused by the new use?	

	Where personal data will be disclosed to a third party: • What types of personal data will be disclosed? • For each type of disclosed data, why is the disclosure necessary? • Will the third party be reminded of the purposes of such disclosure and its responsibility to confine the subsequent use of the data to these purposes? ○ If **no**, please provide justifications.	
DPP4 – Data Security Principle • All practicable steps should be taken to safeguard personal data from unauthorized or accidental access, processing, erasure, loss or use.	Who have access to the personal data collected, and why?	
	Please elaborate the safeguard measures to be implemented to prevent unauthorized or accidental access, process or erasure of personal data, and why the safeguard measures are considered adequate.	
	Where data processor(s) will be involved, please elaborate the controls in place to secure the personal data being handled by the processor(s), and why the controls are considered adequate.	

Areas	PIA Questions	Answers
DPP5 – Openness Principle • All practicable steps should be taken to make known to the public about the organization's personal data policies and practices, types of personal data it holds and the main purposes for which it uses the data.	Is there a privacy policy statement relevant to the present project? • If **no**, please provide justifications.	
	Is the relevant privacy policy statement in compliance with PCPD's Guidance "Personal Information Collection Statement and Privacy Policy Statement"? • If **no**, please provide justifications.	
DPP6 – Data Access and Correction Principle • Data subjects have the right to (i) request access to his/her own personal data held by CMAB, and (ii) request the correction of the personal data supplied in a Data Access Request if it is inaccurate.	Will the data subjects be informed of their right to access and correct their personal data? • If **no**, please provide justifications.	
	Will the data subjects be informed of the post title and the address of the Personal Data Privacy Officer, or the officer who is responsible for handling Data Access Correction Requests? • If **no**, please provide justifications.	
Direct marketing activities	Is the personal data intended to be used indirect marketing activities? • If **yes**, please elaborate how (i) notice will be provided to and (ii) consent will be obtained from the data subjects in accordance with PCPD's Guidance "New Guidance on Direct Marketing" (including notice about the right and method to opt out).	

Part 4: Potential Risks and Mitigation Actions

Based on the results of Part 3, document the privacy risks identified, and the mitigating measures to be/have been taken to reduce the risk to an acceptable level.

Potential risks identified	Mitigation measures

Completed by (Project Owner)	Approved by (IT Security Officer)
Name:	Name:
Post:	Post: IT Security Officer, ITSO, HKUST
Date:	Date:

Please fill in all the required fields in the form and send it to seccomp@ust.hk .

For enquiry, please contact us at seccomp@ust.hk .