Checklist of Best Practice for Mobile App Development by PCPD

This checklist is for mobile application owners or developers to review the handling of sensitive data in their applications. Users are required to complete the checklist with the Best Practice Guide for Mobile App Development from the Office of the Privacy Commissioner for Personal Data (PCPD).

Please complete the document and send it back to ITSC at mobileapps@ust.hk . If the handling of sensitive 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 A - Information of the Mobile Application (the "App")

Application Information	
Name of the App:	
Brief Description of the App:	
App Owner Information	
Name:	
Position:	
Department:	
Email:	

Part B – Checklist of Best Practice for Handling Sensitive Data or Operations

If your app captures or uses any of the data or operations listed in the table below, please review relevant recommendation in the the document, Best Practice Guide for Mobile App Development. Please check the boxes of the related items after you have reviewed the recommendation.

	Data										Operations		
Questions (Please put a tick ☑ in the box after reviewing the proposed recommendation in parentheses)	Unique Device Identifier	Locations	Mobile Phone Number	Contact List/ Address Book	Calendar/ Reminder	Stored Photos/ Videos/ Recordings	SMS/ MMS/ Email Messages	Call Logs	Browser History	App Names/ Account Names	Use Micro-phone/ Camera	Require/ allow user login	Obtain other info*
1. Is the access/ collection/ use of the data absolutely necessary for the app's operation? (See E1)	□	□	□	□	□	□	□	□	□	□	□	□	□
2. Will the data (or derived data) be uploaded/ transmitted from the mobile device? (See E2)	□	□	□	□	□	□	□	□	□	□	□	□	□
3. Will the data (or derived data) be stored or kept elsewhere from the mobile device? (See E3)	□	□	□	□	□	□	□	□	□	□	□	□	□
4. Will the data (or derived data) be combined/ correlated with other data of the individual obtained elsewhere? (See E4)	□	□	□	□	□	□	□	□	□	□	□	□	□
5. Will the data (or derived data) be shared within your business (e.g. for cross-app integration) or with other parties? (See E5)	□	□	□	□	□	□	□	□	□	□	□	□	□
6. Will the data (or derived data) be used for profiling of individual (See E6)	□	□	□	□	□	□	□	□	□	□	□	□	□
7. Will the data (or derived data) be used for direct marketing? (See E7)	□	□	□	□	□	□	□	□	□	□	□	□	□

	Data										Operations		
Questions (Please put a tick ☑ in the box after reviewing the proposed recommendation in parentheses)	Unique Device Identifier	Locations	Mobile Phone Number	Contact List/ Address Book	Calendar/ Reminder	Stored Photos/ Videos/ Recordings	SMS/ MMS/ Email Messages	Call Logs	Browser History	App Names/ Account Names	Use Micro-phone/ Camera	Require/ allow user login	Obtain other info*
8. Has a Personal Information Collection Statement and/or Privacy Policy Statement been prepared to cover all data types involved? (See E8)	□	□	□	□	□	□	□	□	□	□	□	□	□
9. Have you taken into account app users' privacy expectations? (See E9)	□	□	□	□	□	□	□	□	□	□	□	□	□
10. Do you use third-party tools (software library, ad networks etc.) in your app (or are you the provider of these tools)? (See E10)	□	□	□	□	□	□	□	□	□	□	□	□	□

*Note: Please specify the "Other Info" that your mobile app captures in this box.

C. Permission Required in Mobile Application

If your mobile application requires any access permissions (i.e. access to restricted data or actions), please list them in this box.

Please fill in all the required information and send it back to ITSC at mobileapps@ust.hk . For enquiry, please contact us at mobileapps@ust.hk .