香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

PCPD.org.hk

# 開發流動應用程式最佳行事方式指引

# Best Practice Guide for Mobile App Development

# 目錄 Contents

# 目的
# PURPOSE

個人資料私隱保障不應被視為一種只為符規的負擔，反之企業應視之為競爭優勢。本指引旨在為從事開發流動應用程式（「程式」）的人士（包括委託他人開發程式的人士）提供全面及按部就班的實用指引。本指引概述在開發程式時須注意的範疇，以達至尊重客戶的個人資料私隱，從而贏得他們的信任。

由於中小企業可能沒有足夠資源以完全理解其就個人資料私隱保障的法律責任，及自行制訂詳細的程式開發指引，因此，本指引是特別為中小企業提供支援而編製的。

此外，讀者亦應留意程式開發是一個發展迅速的行業，其個人資料私隱保障不單涉及程式，也涉及業務的運作過程。因此依從本指引的建議進行程式開發並未能保證個別程式已完全符合法律要求。

Personal data privacy should not be seen as a pure compliance burden but instead, a competitive advantage a business can build on. This guide aims to provide comprehensive, step-by-step practical guidance to those who are in the mobile applications ("apps") development business (including those who may commission the development of apps). It outlines what areas to pay attention to when developing apps in order to earn trust from customers through respecting their personal data privacy.

This guide is especially tailored for small-to-medium enterprises ("SMEs") which may not have sufficient resources to fully understand their legal obligations, and establish their own comprehensive app development guide taking due account of the importance of protection of personal data privacy.

Readers are also reminded that the app industry is a fast-developing business and personal data privacy protection in apps concerns not only the apps, but also the business's operational processes. Following the recommendations in this guide, therefore, does not guarantee an app is fully compliant with the law.

# 對象
# WHO SHOULD READ

本指引特別為下述人士而設：

1. 程式開發商、委託他人開發程式或決定程式用途的人士（上述人士於本指引統稱為「程式開發商」）；及
2. 向程式開發商提供附加功能代碼的人士，例如廣告網絡或分析工具提供者。如你是代碼提供者，你實際上是向程式開發商提供小型程式，故此你亦應閱覽本指引。

This guide targets specifically the following parties:

1. App developers and those who commission the development of the app or decide on the purpose of the app (collectively referred to as "app developers" in this guide); and
2. Those who provide codes to app developers for added features – such as advertising networks and analytics tool providers. If you are a code provider, you are in effect providing mini-apps to app developers and you too should read this guide.

# 何時閱覽
# WHEN TO READ

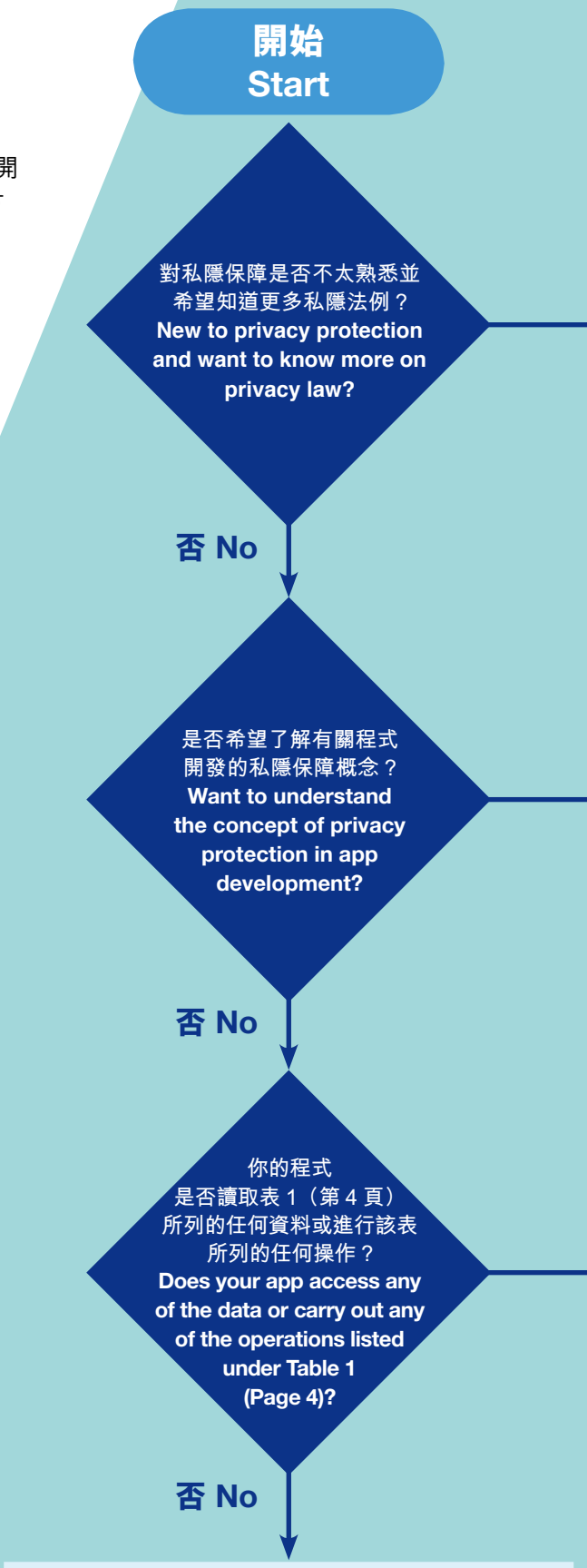
你應在開始計劃開發程式時便閱覽本指引。對企業來說，在開始階段便融入保障私隱的概念，相比日後為符規才作出這方面的調整，前者的花費會較少，而其對程式功能的影響也較為輕微。

You should read it before you start planning your app development project. Building in privacy protection at the outset will be less costly for the business and will have less impact on your app functions compared with adjustment for compliance at a late stage of the project.

# 如何使用本指引
# HOW TO USE THIS GUIDE

為方便參閱，本指引由幾部分組成，每一部分均可獨立閱覽。有關本指引的使用，可參考右面的流程表的建議：

This guide comprises a number of parts which may be read independently. The flow chart on the right suggests how this guide may be used:



是 Yes

**閱讀 A 部 ( 第 6 頁 ) —**
《個人資料（私隱）條例》的相關性
**Read Part A (Page 6) – The relevance of the Personal Data (Privacy) Ordinance**

**閱讀 B 部 ( 第 8 頁 ) —**
法例有甚麼要求？
**Read Part B (Page 8) – What are the requirements under the law?**

是 Yes

**閱讀 C 部 ( 第 11 頁 ) —**
在程式開發中如何執行「貫徹私隱的設計」
**Read Part C (Page 11) – Privacy by Design in app development**

是 Yes

**閱讀 D 部 ( 第 13 頁 ) —**
請填寫 D 部的檢查表，及考慮當中有關的影響
**Read Part D (Page 13) – fill in the checklist in Part D and consider the implications**

**閱讀 E 部 ( 第 17 頁 ) —**
最佳行事方式的建議
**Read Part E (Page 17) – Best practice recommendations**

## 表 1
## TABLE 1

### 擬讀取的資料 Data to be accessed

- 裝置的獨特識別碼
  Unique device identifier
- 定位位置
  Locations
- 機主的流動電話號碼
  Owner's mobile phone number
- 聯絡人 / 通訊錄
  Contact list / address book
- 行事曆 / 提示
  Calendar / reminder
- 儲存的相片 / 短片 / 錄音
  Stored photos / videos / recordings
- SMS / MMS / 電郵訊息
  SMS / MMS / email messages
- 通話紀錄
  Call logs
- 瀏覽紀錄
  Browser history
- 儲存的程式名稱 / 帳戶名稱
  Stored app names / account names
- 儲存的帳戶（任何類別）資料
  Stored account (any type) information

### 擬進行的操作 Operations to be carried out

- 使用流動裝置的麥克風 / 鏡頭
  Using the mobile device's microphone / camera
- 要求 / 容許用家使用登入帳戶名稱登入
  Requiring/allowing user to log on using a login name
- 要求用家提供其他資料
  （姓名、聯絡資料、健康狀況、財務狀況、家庭狀況等資料）
  Requesting app users to provide other details (name, contact details, health, finance, family status, etc.)

# 下一步如何
# WHAT NEXT

當你完成流程表的步驟，你應已有系統地評估你的程式對私隱的影響及作出改善。你應記錄你所作的評估、決定及答案，因為這些資料會提高你對私隱保障的了解。當你需要為你的下一個程式或現有程式的升級版作評估時，這紀錄會是一份很好的參考資料。

After walking through the flow chart, you should have systematically assessed the privacy impact of your app and made the necessary improvements. You should keep a record of your assessments, decisions and answers as they all help to enhance your understanding on privacy protection. This record will be a good reference for you to carry out another assessment on your next or upgraded app.

A 部
Part A

# 條例
# The Ordinance

**《個人資料（私隱）條例》（「條例」）與程式開發有何關係？**
**How relevent is the Personal Data (Privacy) Ordinance (the "Ordinance") to app development?**

A1. 條例規管個人資料的收集、使用、處理、保留、刪除及保安。本指引第 4 頁表 1 所列的任何資料是否屬於個人資料，視乎當這資料連同其他已獲得的資料（如適用）能否識別一個人的身份。

The Ordinance governs the collection, use, processing, storage, erasure and security of personal data. Whether one or more types of the data in Table 1 on page 4 of this guide constitute personal data will depend on whether such data, together with other information available (if applicable) can identify an individual.

A2. 如你收集了一群人的資料，而有些資料可以用來識別部分（但不是所有）個別人士，你仍算收集了個人資料。例如，若你收集程式用家的電郵地址，當中部分電郵地址中的帳號及域名（例如：chantaiman@*pcpd.org.hk*）或許可用以確認某人，而其他地址（例如：chantaiman@*hotmail.com*）或許不能作此用途，但總括來說，你仍算已收集了個人資料。

If you have collected such data from a group of people, and some of it can be used to identify some (but not all) individuals, you should still consider that you have collected personal data. For example, if you collect email addresses from app users, some email addresses (e.g. chantaiman@*pcpd.org.hk*) may be used to identify an individual based on the username and domain name while other addresses (e.g. chantaiman@*hotmail.com*) may not, you should still consider that you have collected personal data.

A3. 若你處理的資料屬條例所定義的個人資料，你的機構及程式必須遵從條例的規定，包括條例附表 1 所列的六項保障資料原則。該六項原則以及與程式開發的關係概要載於 B 部。

If you are dealing with personal data as defined under the Ordinance, your organisation and your app must comply with the requirements under the Ordinance, including the six Data Protection Principles ("DPPs") set out in Schedule 1 to the Ordinance. A brief description of the six DPPs and how they relate to app development can be found in Part B.

**A4.** 嚴格來說，若程式：
**In the strictest sense, if an app:**

a. 只讀取流動裝置內的資料，而不會把資料（或任何源於有關資料的東西）傳輸至其他地方；或
**only accesses data stored on mobile devices and does not transmit the data (or anything derived from the data) elsewhere; or**

b. 沒有把資料用來識別某人；
**has not used the data in a way that may identify an individual;**

該程式開發商未必算是條例所定義的「控制資料的收集、持有、處理或使用」的「資料使用者」。雖然如此，你仍需尊重用家的私隱，清楚告知他們你會讀取甚麼資料及讀取的原因。
**its developer may not be considered a "data user" under the Ordinance who "controls the collection, holding, processing or use of the data". That said, you should still respect users' privacy by clearly informing them what data you would access and why.**

**A5.** 如有人士對某程式作出投訴，條例是否適用取決於有關情況是否涉及個人資料。若你已經依從本指引的建議，便顯示你已在開發程式時謹慎行事，尊重個人資料私隱。若你認為該情況並沒有涉及個人資料，公署仍鼓勵你依從這些建議，以顯示你關心程式用家並願意向他們保證你尊重其私隱。
**If a complaint is lodged against an app, whether the Ordinance will apply to the case will depend on whether personal data is involved. By following the recommendations in this guide, you will be able to demonstrate that you have exercised due care to respect personal data privacy. If you do not think personal data is involved, you are still encouraged to follow these recommendations to demonstrate that you care about the app users and want to assure them that you respect their privacy.**

B 部
Part B

# 六項保障資料原則
# The Six Data Protection Principles

**B1.** 條例下的六項保障資料原則
**The Six Data Protection Principles ("DPPs") under the Ordinance**

B1.1. 保障資料第 1 原則—收集的目的及方式
DPP1 – Purpose and Manner of Collection

B1.1.1. 收集個人資料的目的必須是為了與資料使用者的職能及活動有關而收集；
Personal data shall be collected for a purpose directly related to the function and activity of the data user;

B1.1.2. 就該目的而言，只能收集足夠但不超乎適度的資料；
Only adequate but not excessive personal data is to be collected in relation to the purpose;

B1.1.3. 個人資料須以合法及公平的方法收集；及
Personal data is to be lawfully and fairly collected; and

B1.1.4. 資料當事人須獲告知資料收集及使用的目的。
Data subjects shall be informed of the purpose for which the data is collected and to be used.

B1.1.5. 例如：資料使用者需要通知程式用家收集其個人資料之目的，並應在收集用家個人資料之時或之前（例如在程式安裝時）提供《收集個人資料聲明》，告知他們該程式會收集 / 使用 / 處理甚麼資料。該《收集個人資料聲明》應包涵條例的規定，並提供處理查閱資料或改正資料要求的聯絡詳情（請參閱下文 B1.6 保障資料第 6 原則—查閱及改正）。
For example: In order to inform app users of the purpose of collection, data users should provide a Personal Information Collection Statement to them on or before collection of personal data (such as during the installation process) to tell them what data is to be collected/used/processed through the app. It should also include, among all other requirements under the Ordinance, contact details for data access and correction requests (see also B1.6 DPP6 – Access and Correction below).

B1.2. 保障資料第 2 原則 — 準確性及保留期
DPP2 – Accuracy and Retention Duration

B1.2.1. 資料使用者須採取所有合理並切實可行的步驟以確保：
All reasonably practicable steps shall be taken by the data user to ensure:

B1.2.1.1. 資料被使用時，資料的準確性；及
the accuracy of personal data in relation to its use; and

B1.2.1.2. 資料不會被保存超過該資料被使用於（或會被使用於）的目的所需的時間。
that personal data is not kept longer than is necessary for fulfilment of the purpose for which the data is or is to be used.

B1.2.2. 如聘用資料處理者，資料使用者須確保轉移予該資料處理者的個人資料的保存時間不會超過其就處理該資料所需時間。
When engaging data processors, data users need to prevent any personal data transferred to the data processor from being kept longer than necessary by the data processors.

B1.2.3. 例如：當程式用家刪除程式或要求取消帳戶（如適用）時，你應向程式用家提供選擇，以刪除所有程式及與帳戶有關的資料。
For example: When an app user removes the app or requests an account to be deleted (if applicable), you should offer the app user the option to delete all app-related data and account-related information.

B1.3. 保障資料第 3 原則 — 使用
DPP3 – Use

B1.3.1. 除非資料使用者事前給予同意，否則個人資料只可用於原本收集的目的或直接有關的目的。
Unless the data subject has given prior consent, personal data shall only be used for the purpose for which it is originally collected or a directly related purpose.

B1.3.2. 例如：程式應清楚說明其運作模式，及如其所說明般運作。若所收集的個人資料被用於預定目的之外（例如與其他程式或第三方分享，或與經其他途徑收集的資料串連起來），則需要進行評估，以確定新目的是否與原來資料收集目的直接有關，否則便需取得資料當事人的同意。
For example: An app should clearly say what it does, and only does what it says. If any personal data collected is to be used in a way not envisaged before (such as sharing with other apps or other parties, or combining with other data obtained elsewhere), an assessment needs to be carried out to ascertain if the new purpose of use is directly related to the original purpose of data collection. If not, consent from data subjects should be obtained.

B1.4. 保障資料第 4 原則 — 保安
DPP4 – Security

B1.4.1. 資料使用者須採取所有合理並切實可行的步驟來保障個人資料（包括其交予資料處理者的個人資料），以免受未獲准許或意外的查閱、處理、刪除、喪失或使用所影響，尤其需要考慮到以上情形可能造成的損害。
All reasonably practicable steps shall be taken to ensure that personal data is protected by the data users and its data processors against unauthorised or accidental access, processing, erasure, loss or use having regard to the harm that could result.

B1.4.2. 例如：個人資料的傳輸及儲存應有一定的保障，例如採取加密處理、及以「最小權限」來控制讀取和遵守「有需要才開放」的存取原則。
For example: The transmission and storage of personal data should be protected by measures such as encryption, access control based on “least-privileged rights” and “need-to-know” principles.

B1.5. 保障資料第 5 原則 — 透明度
DPP5 – Transparency

B1.5.1. 資料使用者應制訂及提供有關處理個人資料的政策及措施（包括個人資料的類別及收集目的）予資料當事人。
Data users should formulate and make available to data subjects policies and practices in relation to the handling of personal data (including the types of personal data and the collection purposes).

B1.5.2. 例如：《私隱政策聲明》應可在互聯網上查閱得到，並具體說明你會如何處理儲存於流動裝置或由流動裝置取得的資料。
For example: The Privacy Policy Statement should be readily accessible on the Internet and contain specific coverage on how you would handle data stored on or obtained from mobile devices.

B1.6. 保障資料第 6 原則 — 查閱及改正
DPP6 – Access and Correction

B1.6.1. 資料使用者應根據條例的規定依從查閱資料及改正資料要求。
Data users should comply with data access and data correction requests in accordance with the requirements under the Ordinance.

B1.6.2. 例如： 你應熟悉查閱及改正資料的責任，並設立機制處理這些要求。你的系統設計亦應容許檢索個人資料，以履行有關責任。
For example: You should be familiar with the data access and correction obligations, and establish a mechanism to handle such requests. Your system design should also allow for the retrieval of personal data to fulfil such obligations.

**你現已對法例的要求有所認識，欲了解有關程式開發的私隱保障概念，請參閱 C 部。**
**Now that you have understood the requirements under the law to understand the concept of privacy protection in app development, please read Part C.**

C 部
Part C

# 貫徹私隱的設計
# Privacy by Design

**甚麼意思？**
**What is it?**

在開發一個產品或程式的整個過程中應採納「貫徹私隱的設計」以充分考慮保障私隱的需要。其基本原則有七項[1]。在開發程式方面，主要考慮的範疇如下：
**Privacy by Design is an approach that takes privacy into account throughout the entire development life cycle of a product or process. It is underpinned by seven foundational principles[1]. In the context of app development, the following areas may be considered key factors:**

C1. 減少資料

收集最少量的個人資料（特別是具敏感性的個人資料），是達致「貫徹私隱的設計」的關鍵。若你的程式不會讀取或收集流動裝置的個人資料或任何資料，你便毋須擔心條例中有關收集資料是否合理、程式保障資料及處理查閱及改正資料要求的事宜。若你必須讀取流動裝置的資料或向程式用家收集資料，應考慮收集一般資料而毋須收集精細的資料（例如收集粗略而不是精細的位置、收集年齡而不是收集出生日期）能否達致相同目的。一般來說，你讀取 / 收集 / 使用的個人資料越少，你要擔心的也越少。

Data Minimisation

Reducing the collection of personal data (particularly sensitive personal data) to the absolute minimum is the key element of Privacy by Design. If your apps do not access or collect personal data or any data stored on the mobile devices, you need not concern yourself about the Ordinance in terms of justifying the collection, protecting the data and handling data access and correction requests. If you must access data on the mobile devices or collect the data from app users, consider whether you can achieve the same purpose by collecting general rather than precise data (for example, obtaining approximate instead of precise locations, ages instead of birthdays). In general, the less personal data you access/collect/use, the less you have to worry about.

C2. 避免引起詫異

一般人未必喜歡突如其來的事，故你應公開及坦白地告知用家你會讀取 / 使用甚麼資料（包括儲存於流動裝置或向用家收集的資料），並讓他們適當時有權選擇拒絕。如你把流動裝置的資料與從別處取得的其他資料結合，以用於另一目的，你應考慮這目的是否一個一般非技術性用家會預期的。你亦應評估如此使用資料對用家可能會帶來甚麼不利影響，並消除 / 減低有關影響。

[1] 見 www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf ( 只提供英文版 )
See www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

### Surprise Minimisation

People generally do not like surprises. Be open and frank to users on what information (both stored on mobile devices and gathered from the users) you would access/use, and give them the choice to opt-out from such access/use as they deem appropriate. If you combine mobile device data with other information obtained elsewhere to serve a new purpose, you should consider if the new purpose is normally expected by an average non-technical user. You should also assess the possible adverse effects such use may have on users and eliminate/minimise any such impact.

## C3. 減低風險

如資料會被傳輸及 / 或儲存，就需有足夠保護（即採取加密處理及讀取控制），以確保沒有未經准許的查閱、披露或使用。此外，如對資料作出另類使用（包括在自己業務上或與第三者分享及 / 或在用家不知情下與從別處取得的其他資料結合起來），有關使用必須與原本目的有直接關係，否則須取得有關用家的明確同意。

### Risk Minimisation

If data is being transmitted and/or stored, adequate protection, in terms of encryption and access control, needs to be in place to ensure that there is no unauthorised access, disclosure or use. If additional use of the data is developed (through sharing within your business or third parties and/or combining with other data obtained elsewhere without the knowledge of the user), the use must be directly related to the original purpose of data collection, or else express consent will have to be sought from the users concerned.

## C4. 信任與尊重

即使你認為你的程式所讀取 / 收集的資料不屬個人資料，但告知程式用家你的程式會讀取 / 收集甚麼資料可贏取他們的信任。在流動程式開發方面，這點尤其重要，因為流動裝置載有很多私人資料，程式用家自然十分關心其資料會否在他們不知情下被收集及使用。你可參閱 F 部了解更多的詳情。

### Trust and Respect

Even if you do not think the data your app accesses/collects can be regarded as personal data, telling app users what data your app accesses/collects will earn their trust. This is particularly true when it comes to mobile app development because mobile devices contain a great deal of private information about an individual and app users are naturally greatly concerned that their data is collected and used in ways unbeknown to them. You may wish to read Part F for more details on this.

**你現已對程式開發的私隱保障概念有所認識，如你的程式有讀取第 4 頁表 1 所列的任何資料或進行該表所列的任何操作，你應參閱 D 部考慮當中有關的私隱影響。**

**Now that you have understood the concept of privacy protection in app development and if your app access any of the data or carry out any of the operations listed under table 1 on page 4, you should read Part D to consider the privacy implications.**

D 部
Part D

# 程式開發檢查表
# Application Development Checklist

**如何檢查？**
**How do you check?**

**D1. 基本步驟**
**Basic approach**

D1.1 當在開發程式時採用「貫徹私隱的設計」的方法，程式開發商應對其程式設計作出下述檢查：
Applying the Privacy by Design approach in app development, app developers should perform the following checks on their app design:

D1.1.1. 是否必須讀取流動裝置的資料或從程式用家收集資料？
Is access to data stored on the mobile device or data gathered from app users necessary?

D1.1.1.1. 如必須讀取或收集資料，有沒有清晰的《私隱政策聲明》（或同等文件）向程式用家解釋目的？
If the data access or gathering is necessary, is there a clear Privacy Policy Statement ("PPS"), or equivalent, explaining the purposes of data access or gathering to app users?

D1.1.1.2. 如必須讀取或收集資料，是否有需要將資料上載、儲存、及 / 或分享、將資料與從其他渠道收集的資料結合及 / 或與其他程式或第三方分享資料？
If the data access or gathering is necessary, is it necessary to upload, store and/or share the data, combine the data with other data obtained elsewhere and/or share the data with other apps or other parties?

D1.1.1.3. 如必須讀取、收集、上載、儲存及 / 或分享資料，有甚麼保障措施保護資料免受未獲准許的查閱或使用？
If the data access, gathering, uploading, storing and/or sharing is necessary, what security safeguards are in place to protect the data against unauthorised access or use?

D1.1.1.4. 如必須讀取或收集資料，程式用家是否獲提供途徑以便選擇拒絕並刪除資料？
If the data access or gathering is necessary, has the app user been offered means to opt-out from data access or gathering, and to erase the data?

D1.2. 表 2 的檢查表 ( 第 14 頁 ) 有助你有系統地檢查程式設計，並記錄結果：
Checklist on Table 2 (page 14) has been created to guide and document your checks systematically:

## 表 2 — 檢查表
## TABLE 2 – Checklist

| 問題 Questions | 裝置獨特識別碼 Unique device identifier | 定位位置 Locations | 流動電話號碼 Mobile phone number | 聯絡人 / 通訊錄 Contacts list/address book |
|---|---|---|---|---|
| 1. 是否絕對需要讀取 / 收集 / 使用資料以供程式的運作？見 E1<br>Is the access/collection/use of the data absolutely necessary for the app's operation? See E1 | | | | |
| 2. 會否從流動裝置上載 / 傳輸資料（或衍生資料）？見 E2<br>Will the data (or derived data) be uploaded/transmitted from the mobile device? See E2 | | | | |
| 3. 會否儲存或保留流動裝置的資料（或衍生資料）在別處？見 E3<br>Will the data (or derived data) be stored or kept elsewhere from the mobile device? See E3 | | | | |
| 4. 會否將資料（或衍生資料）與從別處取得的其他個人資料結合 / 串連？見 E4<br>Will the data (or derived data) be combined/correlated with other data of the individual obtained elsewhere? See E4 | | | | |
| 5. 會否在你的業務內分享（例如跨程式整合）或與其他人士 / 機構分享資料（或衍生資料）？見 E5<br>Will the data (or derived data) be shared within your business (e.g. for cross-app integration) or with other parties? See E5 | | | | |
| 6. 會否將資料（或衍生資料）用作建立個人的資料檔案？見 E6<br>Will the data (or derived data) be used for profiling of individuals? See E6 | | | | |
| 7. 會否將資料（或衍生資料）用於直接促銷？見 E7<br>Will the data (or derived data) be used for direct marketing? See E7 | | | | |
| 8. 是否已擬備涵蓋所有資料類別的《收集個人資料聲明》及 / 或《私隱政策聲明》？見 E8<br>Has a Personal Information Collection Statement and/or Privacy Policy Statement been prepared to cover all data types involved? See E8 | | | | |
| 9. 你是否已考慮程式用家在私隱上的期望？見 E9<br>Have you taken into account app users' privacy expectations? See E9 | | | | |
| 10. 你的程式有否使用第三者工具（軟件庫、廣告網絡等）（或你是否這些工具的供應商）？見 E10<br>Do you use third-party tools (software library, ad networks etc.) in your app (or are you the provider of these tools)? See E10 | | | | |

| 資料類別 Types of Data | | | | | | 操作 Operations | | |
|---|---|---|---|---|---|---|---|---|
| 行事曆 / 提示 Calendar/ reminder | 儲存的相片 / 短片 / 錄音 Stored photos/ videos/ recordings | SMS/MMS/ 電郵訊息 SMS/ MMS/email messages | 通話紀錄 Call logs | 瀏覽紀錄 Browser history | 程式名稱 / 帳戶名稱 App names/ account names | 使用麥克風 / 鏡頭 Use microphone/ camera | 要求 / 容許用家登入 Require/allow user login | 提取其他資料 Obtain other info |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

**D2. 檢查表（表 2）的用途：**
**What does Checklist (Table 2) do:**

D2.1. 你應就每類資料或操作回答檢查表（表 2）所列的問題 1 至 10（如有需要可參考 E 部）及將其背後原因記錄在案，這過程有助你有系統地考慮如何在避免侵犯個人資料私隱的情況下設計你的程式。
By answering questions 1 to 10 in Checklist (Table 2) for each type of data or operation (making reference to Part E if needed) and documenting the reasons behind your answers, you are guided to consider systematically how you can build the app with the least intrusion to personal data privacy.

D2.2. 一般而言，問題 1 至 7 及 10 的「√」越少，你的程式侵犯私隱的程度越低。但是「√」的數量並非唯一的衡量準則，因為當涉及較高敏感性的類別，如 SMS/MMS/ 電郵訊息中的「√」對程式用家的影響會大於定位位置中的「√」。因此你應該要小心評估及考慮每個「√」。
As a very general rule, the fewer "√" on the list for questions 1 to 7, and 10, the less privacy intrusive your app will likely be. However, it is not always a simple counting of "√" – the "√" against the storage of SMS/MMS/email messages will have greater impact on app users than the one against access of location information due to the higher sensitivity of the data included in the former category. Each "√" should therefore be carefully assessed and considered.

D2.3. 當你考慮檢查表（表 2）的每個答案時，應審慎地評估你的程式設計是否保障私隱，及在私隱保障或減低程式用家的顧慮方面是否仍有改善空間。
As you develop answers for the questions in the Checklist (Table 2) , you should critically consider if your app design is privacy-friendly, and whether to make improvement in terms of privacy protection or minimisation of potential privacy concerns by app users.

D2.4. 你亦應記錄每個答案背後的原因，這些紀錄有助你向程式用家解釋為何你這樣設計程式。若你日後需要提升你的程式，這份紀錄亦可作為設計參考，提醒你曾經為提高私隱保障而在設計選取了甚麼特點及避免了甚麼步驟。
You should also document the reasons behind each answer as such record will help you explain to app users why you have designed your app in the way it operates. If you need to enhance your app in the future, this record can also be used as a design reference to remind you why you have chosen certain features and avoided other arrangements to stay privacy-friendly to your customers.

E 部
Part E

# 最佳行事方式的建議
# Best Practice Recommendations

**E1.** 只在必要時才讀取 / 收集 / 使用資料
**Only access/collect/use data when necessary**

E1.1. 讓你的程式讀取 / 收集 / 使用每類資料及進行每項操作前，你應先問自己：
Before letting your app access/collect/use each of the data type and carry out each operation, ask yourself:

E1.1.1. 讀取 / 收集 / 使用每類資料的目的是否為程式的性質 / 功能提供支援？
Are the purposes of accessing/collecting/using each type of data to support the nature/functions of the app?

E1.1.2. 要達到這些目的，是否絕對需要讀取 / 收集 / 使用有關資料？
Is it absolutely necessary to access/collect/use the data in order to support the purposes?

E1.1.3. 即使讀取敏感程度較低的資料能否也達致這些目的？
Can the purposes be also supported by accessing less privacy sensitive data?

E1.2. 建議：
Recommendations:

E1.2.1. 若你的程式需要知道程式用家的位置，你可考慮要求用家在知情下在簡圖上指出其位置，而不是自動（及持續地）提取其位置資料；
If your app needs to know the locations of your app users, consider asking users to consciously indicate their locations from a simplified map instead of obtaining their locations automatically and, by definition, continuously;

E1.2.2. 如你必須自動取得位置資料，則應考慮取得約莫的位置資料已可達致你的目的，而毋須精細位置；
If you must obtain location information automatically, consider obtaining approximate locations sufficient to achieve your purpose instead of precise locations;

E1.2.3. 當程式需要傳送具有鑑別碼的 SMS 訊息到流動裝置以確認其電話號碼，程式可能需要讀取 SMS 訊息以協助程式用家自動地填上一次過的鑑別碼。此安排無疑方便了程式用家，讓他不需要鍵入鑑別碼，但此舉亦令程式可以持續讀取其 SMS 訊息；

因此，你應考慮此舉會否引起程式用家在私隱上的不安，或是否可以在 SMS 訊息內提供一個超連結以讓用家可以一按即完成整個鑑別程序；及
In the case where an app needs to send an SMS message with an authentication code to the mobile device in order to confirm the telephone number of the mobile device, the app may require access to the SMS message to intercept the code and activate the verification process automatically. This activation provides convenience to app users so that they do not need to read the SMS message and enter the authentication code manually in the app. However, the app will then be given the right to continuously access all the incoming SMS messages. You should consider whether this will raise privacy concern to app users or whether you can simplify the process by providing a hotlink in the SMS message so that it becomes a 'one-click activation' process; and

E1.2.4. 對於 iOS 程式需要讀取一些並未受其私隱設定獨立保障的資料，或 Android 程式需要讀取資料時，你應考慮在你的程式收集每類資料時，徵求程式用家的准許（及准許用家事後改變主意）或每次都通知他們（例如透過閃爍圖標），以向他們表明該程式只會在有需要時才收集 / 使用有關資料。
For iOS apps where the types of data being accessed are not controlled by the individual privacy setting or for Android apps, you should consider asking permission (and allowing for subsequent changes) from app users or notifying them (e.g. by flashing an icon) each time the data is accessed to demonstrate to them that it would only collect/use the data when it is needed and not continuously.

**E2. 只在有必要時才傳輸 / 上載資料**
**Only transmit/upload data when necessary**

E2.1. 讓你的程式傳輸 / 上載每類資料及進行每項操作前，你應先問自己：
Before letting your app transmit/upload each of the data type and carry out each operation, ask yourself:

E2.1.1. 你傳輸 / 上載資料的目的是甚麼？
What is your purpose of transmitting/uploading the data?

E2.1.2. 要達到這目的，是否絕對需要傳輸 / 上載有關資料？
Is it absolutely necessary to transmit/upload the data in order to achieve the purpose?

E2.1.3. 以傳輸 / 上載資料以外的方式能否也達致同一目的？
Can the purpose be achieved by means other than transmitting/uploading the data?

E2.2. 若必須傳輸 / 上載資料，你應先問自己：
If transmission/uploading of data is necessary, you should ask yourself:

E2.2.1. 資料是否屬於具敏感性，而需要以加密操施，保障傳送安全？
Does the sensitivity of the data being transmitted require protection by encryption?

E2.2.2. 是否已按資料的敏感程度以及最佳行事方式，正確地執行加密措施？
Is the encryption properly implemented according to the sensitivity of the data and best practice?

E2.2.3. 加密操施是否已經涵蓋鑑定技術，以防止較先進的黑客截聽？
Does the encryption implementation include authentication against more advanced hacking?

E2.3. 建議：
Recommendations:

E2.3.1. 若你需要把資料上載到後端伺服器，以查閱其他資料繼而再下載至程式（例如根據程式用家位置查閱最就近分行地址），你可考慮（如速度及資料容量許可）先下載數據到流動裝置才進行查閱；及
If you need to upload data to the backend server in order to look up results to download to the app (e.g. looking up the nearest branch address based on the app user's location), you may consider (if speed and data volume allow) preloading the results and carrying out the look up function on the mobile device instead; and

E2.3.2. 取而代之，你亦可考慮先概閱資料（例如把精細位置轉換成十八區中的其中一區）再上載區域資料到伺服器查閱。
Alternatively, you may consider doing a simple look-up first (e.g. mapping precise locations to one of the 18 districts), before uploading the district data to your server for further look up.

E2.3.3. 若要傳輸敏感資料，而需要加密保護時，你應該確保妥善加密，例如使用複雜的加密運算、檢查電子證書是否依然生效並由認可的機關核證，亦要考慮加設證書鑑定技術，以確保傳輸資料受到應有的保護。詳情請參考「流動應用程式 (SSL 實施 ) 最佳行事指引」[2]。
If the sensitivity of the data being transmitted requires encryption, you should implement the encryption properly including the use of strong algorithm, checking for certificate expiry date and signing authority, as well as considering adding authentication techniques such as certificate pinning to ensure the data being transmitted is properly protected. You may refer to the *Best Practice Guide (SSL Implementation) for Mobile App Development*[2] for professional advice.

**E3. 只有在必要時，才把資料儲存 / 保留在流動裝置以外的地方**
**Only store/keep data elsewhere from the mobile device when necessary**

E3.1. 讓你的程式儲存 / 保存每類資料及進行每項操作前，你應先問自己：
Before letting your app store/keep each of the data type and carry out each operation, ask yourself:

E3.1.1. 把資料儲存 / 保存在流動裝置以外的地方，目的是甚麼？
What is the purpose of storing/keeping the data elsewhere from the mobile device?

[2] 由香港電腦保安事故協調中心及香港專業資訊保安協會聯合出版 :www.hkcert.org/my_url/zh/guideline/15091401
Published jointly by the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and the Professional Information Security Association of Hong Kong (PISA): www.hkcert.org/my_url/guideline/15091401

E3.1.2. 是否絕對需要在流動裝置以外的地方儲存 / 保存有關資料以達致這些目的？
Is it absolutely necessary to store/keep the data elsewhere from the mobile device in order to achieve the purpose?

E3.1.3. 用其他方法能否也達致這些目的？
Can the purpose be achieved by other means?

E3.1.4. 儲存在別處的資料是否有足夠的保護，例如在「有需要原則」下控制讀取資料及 / 或加密處理？
Is there adequate protection over the stored data residing elsewhere, for example, with "need-to-know" access control and/or encryption?

E3.1.5. 你有否為程式用家提供移除 / 刪除該儲存資料的途徑？
Have you provided any means for app users to remove/erase the stored data?

E3.2. 建議：
Recommendations:

E3.2.1. 若程式在每次運作時，都會上載用家最新的通訊錄到伺服器中使用，你應考慮把伺服器中不再需要的通訊錄資料盡快刪除；
If you need to upload and use the latest copies of the user's contact list every time your app runs, consider erasing the contact list stored in the server as soon as it is no longer needed;

E3.2.2. 若你需要保存用家最新的通訊錄在伺服器內，但只使用其電話號碼，應考慮刪除已保存於通訊錄中的姓名 / 名稱欄目；及
If you need to keep the latest copies of the user's contact list in the server but are only using the telephone numbers, consider erasing the name/label fields of the stored contact lists; and

E3.2.3. 你應考慮向程式用家提供途徑以刪除儲存在流動裝置及後端伺服器的資料（包括任何帳戶或帳戶相關資料），此選擇對於希望從其流動裝置中移除你的程式的程式用家尤其重要。
You should consider providing a means for app users to delete the data (including any account or account related data) stored on the mobile device and in backend servers, particularly when the app users wish to remove your app from their mobile devices.

**E4. 只在適當情況 ( 詳情參考 E4.1) 才把程式用家的資料與從別處取得同一用家的其他資料結合 / 串連起來（例如當用家以社交網站帳戶登入你的程式，你便可以把程式提供 / 收集的資料與從別處取得有關該社交網站帳戶的其他資料結合 / 串連）。**
**Only combine/correlate data with other data of the app user obtained elsewhere when it is appropriate (see E4.1) (for example, when users log on to your app using a social network account, you could then combine/correlate app data with data available/obtained relating to that social network account).**

E4.1. 把程式用家的資料與從別處取得的用家資料結合 / 串連前，你應先問自己：
Before combining/correlating the data with other data of the app user, ask yourself:

E4.1.1. 把程式用家的資料與從別處取得的用家資料結合 / 串連的目的是甚麼？有關目的是否與原本的資料收集目的相同或直接有關？程式用家是否知道、同意及 / 或可選擇拒絕這結合 / 串連資料的做法？

What is the purpose of combining/correlating the data with other data of the app user obtained elsewhere? Is the purpose of combining/correlating the data the same as or directly related to the original purposes of accessing/collecting the data and the other data? Do app users know, agree to and/or have the choice to opt-out of such combination/correlation?

E4.1.2. 是否絕對需要結合 / 串連資料以達致這目的？
Is it absolutely necessary to combine/correlate the data in order to achieve the purpose?

E4.1.3. 能否以其他方法達致結合 / 串連資料這目的？
Can the purpose be achieved by means other than combining/correlating data?

E4.1.4. 你有否採取步驟以防止不當或不正確的資料結合 / 串連？有否考慮如果結果出錯將會有甚麼不利的影響？
Have you taken steps to prevent inappropriate/incorrect combination/correlation? What would be the adverse effect of such an error?

E4.2. 建議：
Recommendations:

E4.2.1. 若你把程式用家的資料與從別處取得的有關同一用家資料結合 / 串連，你應告知程式用家有關的詳情，並容許程式用家可選擇拒絕此結合 / 串連的安排；
If you do combine/correlate an app user's data with other data of the same user, you should consider informing app users of the details. You should also consider allowing app users to opt-out from having their data combined/correlated;

E4.2.2. 你應考慮容許程式用家匿名地使用你的程式（即毋須先登入帳戶）；及
You should consider allowing app users to use your app anonymously without logging in; and

E4.2.3. 你應顧及到用家有可能更改電話號碼，因此你不應只用電話號碼以提取儲存的用家的資料，以免某人的資料因其更換電話號碼而被他人提取。
You should consider the possibility of users changing their phone numbers. You should therefore not use the telephone number alone to retrieve stored data to prevent data related to one person from being retrieved by another because of change of phone number.

**E5. 只在適當情況 ( 詳情參考 E5.1) 才在企業內或與其他人士分享收集得的資料**
**Share the data within your business or with other parties only if appropriate (see E5.1)**

E5.1. 在分享資料前，你應先問自己：
Before sharing the data, ask yourself:

E5.1.1. 分享資料的目的是甚麼？是否與原本資料讀取 / 收集目的相同或有直接關係？此外，程式用家是否知道、同意及 / 或可以選擇拒絕資料被如此分享？

What is the purpose of sharing the data? Is it the same as or directly related to the original purpose of accessing/collecting the data? Do app users know, agree to and/or have the choice to opt-out of such sharing?

E5.1.2. 是否有絕對需要在你的企業內及 / 或與其他人士分享資料？
Is it absolutely necessary to share the data collected within your business and/or with other entities?

E5.1.3. 能否以其他方法以達致分享資料要達到的目的？
Can the purpose of the sharing be achieved by means other than sharing the data?

E5.1.4. 若分享資料是與其他公司的直銷活動有關，你是否肯定如此分享符合條例的規定？
If the sharing is related to direct marketing by other parties, have you confirmed whether such sharing is in compliance with the requirements under the Ordinance?

E5.2. 建議：
Recommendations:

E5.2.1. 若你沒有清楚告知程式用家，不應把從一個程式所收集的資料與你從另一個程式或另一來源所收集同一程式用家的資料結合，以圖分析程式用家的行為或喜好；及
If you have not made it clear to app users, you should not combine data collected from one of your apps with data of the same app user collected from another app of yours, or other sources, to study the behaviour or preference of app users; and

E5.2.2. 即使你認為你的程式沒有收集程式用家的個人資料，在與另一方分享資料前，應考慮進行私隱風險評估，因為你未必知道另一方會否及能否可匯集有關的資料以識別個別人士。
Even if you believe you have not obtained app users' personal data through your app, you should still consider carrying out a privacy risk assessment before sharing any data of the users with outside parties. This is because you do not know what other data these outside parties may have, and whether in aggregate they are capable of identifying the individuals.

**E6. 在利用資料建立個人資料檔案要具透明度**
**Be transparent if you use data for profiling individuals**

E6.1. 在你使用程式用家的資料來建立個人資料檔案前，應先問自己：
Before the data is used for profiling app users, ask yourself:

E6.1.1. 建立程式用家個人資料檔案的目的是甚麼？這目的是否與原本的資料讀取 / 收集目的相同或直接有關？程式用家是否知道、同意及 / 或可以選擇拒絕這樣的做法？
What is the purpose of profiling app users? Is the purpose of profiling the same as or directly related to the original purpose of accessing/collecting the related data? Do app users know, agree to and/or have the choice to opt-out of such profiling?

E6.1.2. 是否有絕對需要建立程式用家個人資料檔案以達致這目的？
Is it absolutely necessary to profile app users in order to achieve the purpose?

E6.1.3. 能否以其他方法達致建立程式用家個人資料檔案這目的？
Can the purpose be achieved by means other than profiling app users?

E6.1.4. 你有否評估建立程式用家個人資料檔案所帶來的影響以及採取步驟以防止建立個人資料檔案可能引起的不理想後果？
Have you assessed the adverse consequence of profiling and taken steps to prevent profiling with undesirable outcomes?

E6.2. 建議：
Recommendations:

E6.2.1. 若所讀取 / 收集的資料是用作建立程式用家個人資料檔案，你應 (1) 告訴程式用家你用其甚麼資料來組成其個人資料檔案，及 (2) 容許程式用家拒絕有關安排；及
If data accessed/collected is used for profiling app users, you should (1) tell them what data you use for what profiling purpose, and (2) allow them to opt out of the arrangement; and

E6.2.2. 若所讀取 / 收集的資料是用作對某類型程式用家的市場分析，你應向程式用家保證，你的分析並不會以個別用家為對象，或建立他們個人的資料檔案。
If data accessed/collected is used for gauging the collective preference of groups of app users, you should assure app users that you will not use the data to profile or target them individually.

**E7. 你使用目標客戶的個人資料進行直接促銷前必須取得對方同意**
**You must obtain consent from target customers before using their personal data for direct marketing**

E7.1. 你在使用所收集的個人資料作直接促銷用途前，應先問自己：
Before personal data is used for direct marketing purposes, ask yourself:

E7.1.1. 你是否肯定已經依從條例的規定給予目標客戶有關通知及已經得到他們的同意？
Are you sure you have followed the prescribed procedures for notifying the target customers and obtaining their consent in accordance with the requirements under the Ordinance?

E7.2. 建議：
Recommendations:

E7.2.1. 若你有意使用所讀取 / 收集的個人資料作直接促銷用途，你應遵從條例第 VI A 部及專員發出的《直接促銷新指引》[3]。
If you intend to use the personal data accessed/collected for direct marketing purpose, you should comply with Part VI A of the Ordinance and the *"New Guidance on Direct Marketing"* [3] published by the Commissioner.

[3] 請參閱 www.pcpd.org.hk/tc_chi/resources_centre/publications/guidance/files/GN_DM_c.pdf
Please see www.pcpd.org.hk/english/resources_centre/publications/guidance/files/GN_DM_e.pdf

## E8. 你的《收集個人資料聲明》及《私隱政策聲明》應具透明度
## Be transparent in your Personal Information Collection Statement ("PICS") and Privacy Policy Statement ("PPS")

E8.1. 使用每種類別資料及執行不同的運作前，應先問自己：
For each of the data types you will use and the operations you will perform, ask yourself:

E8.1.1. 你是否已經以易於理解的方式在《私隱政策聲明》中向程式用家解釋為何你的程式需要讀取 / 傳輸 / 儲存 / 分享 / 使用有關資料？如果你要使用該應用程式的資料在其他用途上，你是否已經在《私隱政策聲明》中解釋清楚？
Have you explained in the PPS, in an easily understandable manner, to the app users why your app needs to access/transmit/store/share/use the data? If your business makes use of the data beyond the app, have you explained it in the PPS why you need to so use the data?

E8.1.2. 為向程式用家保證你尊重其私隱，你是否應該不單向他們解釋你會如何處理資料，亦應考慮表明不會把資料用於其他可能構成私隱風險的用途上？
To assure app users that you respect their privacy, should you explain not only what you will do with the data, but also what you will not do with the data that may cause privacy concerns?

E8.1.3. 你是否知道《收集個人資料聲明》（你向程式用家收集個人資料之時或之前必須向他們提供的聲明）與《私隱政策聲明》（表明你會如何處理個人資料的一般聲明）的分別，及在哪些情況下應向用家提供哪一份聲明[4]？
Do you understand the difference between PICS (which must be provided to app users when or before you collect personal data from them) and PPS (a general statement to tell people how you would handle personal data) and know which one you should provide to app users in varying circumstances[4]?

E8.2. 建議：
Recommendations:

E8.2.1. 你應利用「程式安裝」頁面預設的私隱政策連結，在程式用家安裝程式前解釋你的程式及業務（如適用）會讀取 / 傳輸 / 儲存 / 分享 / 使用甚麼資料及其原因；
You should make use of the default Privacy Policy link in the app installation page to explain to app users, prior to the installation of the apps, what data your app, and where applicable, your business, would access/transmit/store/share/use and why;

E8.2.2. 若私隱政策過於複雜，可考慮以分層方式呈示，在一頁或幾頁上呈示基本 / 主要資料，再以適當連結提供詳情。同樣地，你可考慮用圖標、圖形或動畫把私隱政策簡化；及
If the privacy policy is complicated, consider using a layered approach to explain the details, with the basic/essential details summarised on a single or a few pages, and further details

[4] 請參閱《擬備收集個人資料聲明及私隱政策聲明指引》www.pcpd.org.hk/tc_chi/resources_centre/publications/guidance/files/GN_picspps_c.pdf
Please see *Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement*: www.pcpd.org.hk/english/resources_centre/publications/guidance/files/GN_picspps_e.pdf

provided through appropriate hyperlinks. You may also consider the use of icons, graphics or animations to simplify the privacy policy for app users; and

E8.2.3. 若你需要用家授權你讀取一系列的資料，但其實你只需要系列中的部分資料以達致你的目的，你應考慮在《收集個人資料聲明》及 / 或《私隱政策聲明》中清楚表明你不會讀取 / 使用系列中的某些其他資料。
If you need a user to grant you the right to access a range of data but in fact you only need to use part of that data range, you should consider making it clear in your PICS and/or PPS what data you would not access/use.

**E9. 你應從程式用家的私隱期望角度考慮程式的設計**
**You should take into account app users' privacy expectations**

E9.1. 如你能夠從程式用家的角度去設計程式，可以緩解他們很多私隱上的顧慮：
It will go a long way to alleviate app users' privacy concerns if you design the app to take account of their expectations:

E9.1.1. Android 作業系統會在程式用家安裝程式前呈示「權限」頁面。你應該確保你已從程式用家的角度閱讀「權限」頁面。你應考慮當你的程式讀取的權限超越用家根據程式的表面功能所得出的預期，用家會否對使用你的程式有所保留；及
In the case of Android, app users are presented with a Permission Page prior to installing the app. Make sure you have read the permission page from the viewpoint of an app user. Consider if the user will be concerned if your app seeks permissions for data access that exceed the user's normal expectation based on the app's apparent functions; and

E9.1.2. 至於 iOS 作業系統，即使程式用家不獲呈示「權限」頁面，他們仍然可以經由 iOS 私隱設定控制得知你的程式所需的部分權限。同樣地，你亦應該考慮當你的程式讀取的權限超越用家根據程式的表面功能所得出的預期，用家會否對你使用的程式有所保留。
In the case of iOS, even if app users are not presented with a Permission Page, they will still find out if the app will access some of the data controlled by the Privacy Setting of iOS. Again consider if the user will be concerned if your app seeks permissions that exceed the user's normal expectation based on the app's apparent functions.

E9.2. 建議：
Recommendations:

E9.2.1. 檢視你的 Android 程式的「權限」頁面，看看所讀取的權限對一般用家而言是否合理。對首次使用的用家來說，他們可能會未能察覺你的程式中有某些特點，但這些特點正正就是需要使用某些特別權限的原因。向用家解釋這些特點與讀取權限的因果關係並不費勁，但卻可贏取他們的信任；
Look at the Permission Page of your Android app and ask yourself if the permission sought for data access looks reasonable to the average user. Your app may have some special features that are not apparent to first-time users but justify the permission sought. The effort to explain why your app needs such permission is small but goes a long way to earn trust from your users;

E9.2.2. 如你的升級程式較舊版需要讀取及/或收集更多類別的資料，Android 作業系統會在更新前向程式用家指出這些差異，及要求程式用家確認使用/接受。你應小心解釋需要讀取更多資料的原因，向程式用家解釋你不是因為他們慣於使用你的程式的舊版本而「走後門」地利用更新版本去讀取他們更多的個人資料；及
If your updated app requires access to and/or collects more types of data than its older version, Android will highlight the difference to app users prior to the updating and ask for their confirmation. You should carefully explain the reasons of the needed access so that app users will not think that you are trying to access more of their personal data "by the back door" after they have got used to using the earlier version of your app; and

E9.2.3. 審閱你的 iOS 程式及檢視甚麼時候 iOS 作業系統會要求用家容許程式查閱個別的資料，以判斷程式是否已經解釋清楚，讓用家明白為何需要這些權限。例如程式在初始化時需要讀取位置資料（但程式不會即時顯示與位置有關的結果），程式用家就可能質疑程式使用位置的原因。
Walk through your iOS app to see when permission would be brought to the attention of the users and determine if sufficient explanation has been given to them why you need the access. For example, if your app requires access to location to initialise functioning (but the results related to the access of location are not displayed immediately), app users may wonder why your app requires access to locations upfront without good reason.

**E10. 使用、包含或供應第三方的程式研發工具時要具透明度**
**Be transparent if you use, include or provide third-party app-development tools**

E10.1. 若你在程式中使用或包含第三方工具（例如軟件庫及廣告網絡/廣告工具）或是供應這些工具，你亦應考慮下述事宜：
If you use or include third-party tools (such as software library and advertisement network/advertisement tool) or provide such tools, you should consider the following:

E10.1.1. 若你的程式使用或包含第三方功能/工具，你應查看這些工具對程式用家的個人資料私隱有否任何影響。有些工具會透過監察流動裝置的識別碼，甚至裝置內儲存的其他帳戶資料，追蹤程式用家的行為。雖然這些資料不是由你直接讀取/收集，但資料是經由你的程式為第三方收集。因此，你應該清楚了解這些工具如何運作、評估使用並羅列這些工具的影響，以及將詳情告知你的程式用家；及
If you use or include third-party functions/tools in your app, you should find out if such tools have any personal data privacy impact on your app users. Some tools may track app users' behaviour by monitoring the unique identifier of the mobile devices or even details of other accounts stored on the mobile device. Although such data is not accessed/collected by you directly, it is being collected through your app for these third-parties. You should therefore find out how these tools operate, assess the impact of using/including them, and tell your app users the purposes of such access/collection; and

E10.1.2. 若你向其他開發商供應這類第三方工具，你應該告知他們，你的工具需要甚麼權限去閱讀資料及其原因。若你收集這些資料作自用，除了告知有關開發商收集資料的種類及目的外，你亦應向程式用家提供拒絕如此收集的途徑。
If you are providing third-party tools to other developers, you should let them know what permissions your tools require in order to access data and why. If you are collecting any of such data for your own use, apart from informing developers the types of data collected and the purposes for collection, you should offer app users the means to opt-out of such collection.

E10.2. 建議：
Recommendations:

E10.2.1. 若你在程式中使用或加入的第三方工具，而對方沒有告知你會自行讀取 / 收集資料（因此程式用家亦會不知情），此類讀取 / 收集或會出乎意料地出現在用家的「權限」頁面上。你應檢查你的程式在最後「權限」頁面上的顯示，確保用家不會因突然發現而感到詫異；
If third-party tools you have used to develop or have included in your apps are accessing/collecting data for themselves without telling you (and therefore app users), such access/collection may show up on the Permission Page out of your users' expectation. You should therefore check the Permission Page of your app that uses third-party tools and make sure there are no unexpected surprises;

E10.2.2. 若你計劃採用第三方提供者的內置廣告，你應該向他們查問會否透過你的程式對程式用家進行追蹤 / 建立個人資料檔案。如有，你應該了解詳情，並向你的程式用家解釋廣告網絡會作甚麼形式的追蹤 / 建立怎樣的個人資料檔案。你亦應該向第三方了解程式用家是否可以拒絕此安排；及
If you plan to deploy in-app advertising from third-party providers, you should find out from them if they carry out tracking/profiling of app users via your app. If affirmative, you should find out the details and explain to your app users what tracking/profiling the advertising network will do. You should also find out if there is a way for app users to opt out; and

E10.2.3. 你須知道，由於是你選擇及決定採用某廣告網絡，故此你同樣需要就他們收集資料的做法負責。
You should note that since you have made a decision to use a particular advertising network, you are equally responsible for their collection of data.

F 部
Part F

# 不讀取 / 收集資料的程式的最佳行事方式建議
# Best Practice Recommendations for Apps that do not Access/Collect Data

**F1.** 不讀取 / 收集資料的程式的最佳行事方式建議
**Best practice recommendations for apps that do not access/collect data**

F1.1. 透明度 Transparency

F1.1.1. 即使你的程式並不讀取 / 收集流動裝置內任何資料或從程式用家提取資料，公署仍強烈建議你在程式安裝前向程式用家呈示《私隱政策聲明》，向用家表明你的程式不會讀取 / 收集他們任何資料，以建立他們對使用你的程式的信任。
Even if your app does not access/collect any data stored on the mobile device or obtain information from app users, you are still strongly advised to display to the app user before app installation a privacy policy statement to this effect. This proactive strategy will enhance user's trust in using your app.

F1.2. 建議：
Recommendations:

F1.2.1. iOS 程式並沒有「權限」頁面向程式用家呈示程式會否讀取 / 收集甚麼資料。如你研發了一個 iOS 程式，而該程式無需讀取流動裝置內任何資料或從程式用家提取資料，你應在私隱政策中向用家清楚表明；及
For example, in the case of iOS apps, there is no permission page to show app users what data an app would access/collect. If you have developed an iOS app which does not require access to any data on the mobile device or obtain data from app users, you should still say this clearly in a privacy policy for the benefit of the users; and

F1.2.2. 要是你設計的是 Android 程式，即使它沒有讀取流動裝置內任何資料或從程式用家提取資料，「權限」頁面或會呈示程式需要的其他權限（例如網絡連接）。為向程式用家作出保證及建立其信任，你亦應在私隱政策中清楚表明需要有關權限的目的或向程式用家表明你的程式不會讀取或需要讀取任何資料。
In the case of Android apps, even if your app does not access any data on the mobile device or obtain data from app users, the Permission Page of the app may or may not show other permissions required (e.g. network connection). In order to assure and build trust with app users, you should still clearly say in a privacy policy what those permissions are and why they are needed, and that your app does not access or need to access any data.

# 鳴謝
# ACKNOWLEDGMENT

香港無線科技商會對本指引的編製提供寶貴意見及支援，個人資料私隱專員公署謹此鳴謝。

The Office of the Privacy Commissioner for Personal Data wishes to thank the Hong Kong Wireless Technology Industry Association in providing valuable advice and support in the preparation of this Guide.

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

PCPD.org.hk


查詢熱線 Enquiry Hotline : (852) 2827 2827
傳真 Fax : (852) 2877 7026
地址 Address : 香港灣仔皇后大道東 248 號
陽光中心 12 樓
12/F, Sunlight Tower,
248 Queen's Road East,
Wanchai, Hong Kong
電郵 Email : enquiry@pcpd.org.hk





二零一四年十一月初版
First published in November 2014

二零一五年十月（第一修訂版）
October 2015 (First Revision)