視察報告

（根據香港法例第 **486** 章《個人資料（私隱）條例》
第 **48(1)**條發表）

香港私營補習服務行業的

個人資料系統

報告編號：R18 – 13069

2018 年 **12** 月 **28** 日

本頁面乃故意留空以便雙面打印

香港私營補習服務行業的個人資料系統視察報告

香港個人資料私隱專員根據香港法例第 486 章《個人資料（私隱）條例》第 36 及 48 條行使賦權對香港私營補習服務行業的個人資料系統的視察發表報告。

條例**第 36 條**規定：

「*在不損害第 38 條的概括性原則下，專員可對－*

(a) 資料使用者所使用的任何個人資料系統；或

(b) 屬於某資料使用者類別的資料使用者所使用的任何個人資料系統，

進行視察，目的在確定資訊以協助專員－

(i) 在－

(A) (a)段適用時，向有關的資料使用者；

(B) (b)段適用時，向有關的資料使用者所屬於的一個類別的資料使用者，

作出建議；及

(ii) 作出關於促進有關的資料使用者或有關的資料使用者所屬於的一個類別的資料使用者（視屬何情況而定）遵守本條例的條文（尤其是各保障資料原則）的建議。」

根據條例**第 2(1)條**，「**個人資料系統**」是指「*全部或部分由資料使用者用作收集、持有、處理或使用個人資料的任何系統（不論該系統是否自動化的），並包括組成該系統一部分的任何文件及設備。*」

條例**第 48 條**的有關部分規定：

「*(1) 在符合第(3)款的規定下，專員在第 36(b)條適用的情況下完成一項視察後，可－*

(a) 發表列明由該項視察引致的、專員認為是適合作出的關乎促進有關資料使用者所屬的某類別資料使用者遵守本條例條文（尤其是各保障資料原則）的任何建議的報告；及

(b) 以他認為合適的方式發表該報告。

…

(3) 除第(4)款另有規定外，根據第(1)款...發表的報告的擬訂形式，須以防止可從報告中確定任何個人的身分為準。

(4) 第(3)款不適用於屬以下人士的個人 —

(a) 專員或訂明人員；

(b) 有關資料使用者。」

香港個人資料私隱專員　黃繼兒

2018 年 12 月 28 日

視察報告
（根據香港法例第 486 章《個人資料（私隱）條例》第 48(1)條發表）

香港私營補習服務行業的個人資料系統

摘要

背景

1. 香港，如同中國大陸、日本及台灣等其他亞洲主要法域區，非常著重學童[1]的學業成績及公開考試成績。因此，私營補習服務百花齊放，私營補習機構的大型廣告比比皆是，成為學童在傳統學校外獲得學業知識的主要渠道。根據調查資料顯示，超過 76%學童曾接受私營補習服務，當中 22%學童早於小學四年級起已經開始接受這類輔導教育。

2. 香港個人資料私隱專員（**私隱專員**）非常重視學童的個人資料私隱。由於學童對私隱的意識偏低，傾向依從指示及十分容易受朋輩影響，因此私隱專員認為以學童為服務對象的機構應對這個群組人士特別給予私隱保障。

3. 私營補習行業服務種類繁多，處理的個人資料不但數量龐大，亦涉及敏感的個人資料。私隱專員認為現時審視私營補習行業在保障個人資料私隱這個範疇的運作，符合公眾利益。因此，私隱專員根據香港法例第 486 章《個人資料（私隱）條例》（**條例**）第 36 條對三所私營補習機構的個人資料系統進行視察（**本視察**）：

   (i) 一所連鎖式經營的補習機構；
   (ii) 一所以特許經營模式營運的補習機構；及
   (iii) 一所利用網上媒體（流動應用程式）提供補習服務的機構。

4. 本視察覆蓋上述三種不同營商模式的私營補習機構在處理個人資料的整個流程。私隱專員從本視察中了解到他們對處理個人資料存有不同的理念及認知，導致他們的個人資料系統在不同方面各有長短。專員期望在本視察所得出的視察結果及建議能讓業界完善其私

[1] 在本報告中「學童」指 18 歲以下人士

隱保障的政策及運作常規，建立「保障與尊重個人資料私隱」的文化，並協助他們遵從條例及條例附表 1 的保障資料原則的規定。

視察結果及建議

5. 在本視察中，私隱專員注意到該三所機構在實際的營運過程及常規中，均有採取保障個人資料的措施。雖然該三所機構所採取的個人資料保障措施大致上可以接受，但從個別機構的職能中仍反映不足之處。私隱專員認為，負責任的機構的最佳行事方式是建立及全面執行「私隱管理系統」[2]。私隱管理系統應涵蓋整體業務常規、操作程序、產品和服務設計、實體建築，以至網絡基礎設施。在策略層面，機構可採用私隱管理系統作為框架，輔以恒之有效的檢討及監察程序，建立健全的私隱保障基建，藉以配合機構遵從條例的規定。

6. 本視察顯示該三所機構已致力進行私隱管理。他們的個人資料系統在各方面互有長短，仍有不少改善空間。除了條例的規定外，私隱專員亦參照一個全面的私隱管理系統的要求，對私營補習市場的機構提出下述建議，以提升企業問責性，並與顧客建立互信的基礎，以期在處理私隱的過程達至雙贏的局面：

(1) 將私隱保障納入企業管治

私隱專員注意到其中一所機構未有將個人資料私隱保障納入企業管治。私隱專員強烈鼓勵所有私營補習機構（不論其營商模式或機構大小）應將個人資料私隱保障納入企業管治，並對此作出機構性的承諾；從最高管理層中委任保障資料主任，以管理私隱管理系統及資料保障相關事務，並在機構建立專重私隱的文化。

(2) 貫徹私隱的設計

私營補習機構在設計新產品及服務時，應寓私隱保護於設計之中，並評估推出新產品及服務對個人資料私隱的影響。機構可有效利用資訊科技工具，以顧客為本，將私隱外洩風險降低。

[2] 專員於 2014 年 2 月出版了一份《私隱管理系統：最佳行事方式指引》，扼述如何建立專員所提倡的健全私隱管理系統。

(3) 制定全面的私隱政策

私隱專員注意到該三所機構皆沒有全面的機構性私隱政策。不論營商模式或機構大小，私營補習機構應就其處理個人資料的措施制定全面的私隱政策。有關的私隱政策必須適用於所有部門及補習中心，亦必須適時通知所有員工有關規定，以確保機構對處理個人資料的制度及措施一致。為配合社會及業務發展，機構亦應定期檢討及更新其私隱政策。

私隱政策應涵蓋個人資料（包括文件及電子記錄）收集、準確性、保存期限、使用、保安措施、銷毀程序，以及處理直接促銷活動及拒收訊息的要求及操作程序等各項範疇。

由於現時處理補習服務非常倚重資訊科技，安全的資訊科技系統尤為重要。私營補習機構應就資訊科技保安制定相關政策，訂明機構所有採取的資訊科技保安措施及應對相關保安風險的實務政策。

(4) 建立有效的匯報系統及資料外洩事故通報機制

私隱專員注意到其中兩所機構沒有書面指引或程序，規管處理資料遺失或外洩的情況。為應對處理個人資料私隱的各項事宜，私營補習機構應建立一套有效的匯報及監控系統，，以能適當地回應處理個人資料時所帶來的問題，並確保員工遵從機構制定的私隱政策。

私營補習機構應制定資料外洩事故的通報機制，訂明處理此等事故的流程（包括如何遏止資料外洩及減少損失的即時評估及補救措施），並委派指定管理層負責處理此等情況。

(5) 透過培訓及教育提升員工對私隱保障的意識

私隱專員注意到其中兩所機構只會向新入職員工提供有關個人資料私隱的培訓。為建立員工對私隱保障的意識及機構的尊重私隱文化，私營補習機構應定期提供教育及培訓予所有員工（包括特許經營人士及其員工或其他營商模式旗下的員工）。個人資料保障的全面培訓及複修課程不限於專門培訓

課程、電郵或機構通訊內的實用提醒，以至內聯網內提供相關的資訊內容等。

(6) 停止不必要或過量收集個人資料

私隱專員注意到其中兩所機構涉及過量收集個人資料，而當中的一所機構亦未有在其申請表格內提供個人資料收集聲明。私營補習機構應檢視其收集個人資料的情況，尤其需考慮以下因素：

(i) 如發現涉及收集過量或不必要的個人資料的情況，立即停止如此收集的行為，修訂相關表格並刪除或銷毀已收集的個人資料；
(ii) 在登記或申請表格上提供個人資料收集聲明，以通知學童及其家長有關的收集目的及保障資料第 1(3)原則所訂明的其他情況；及
(iii) 因應服務的性質，盡量減少收集個人資料的種類。

(7) 避免永久保留個人資料

永久保留個人資料會違反條例第 26 條及資料保障第 2(2)原則。私隱專員對該三所私營補習機構在不同情況下採取了永久保留學童或導師的個人資料的做法感到失望。私營補習機構應訂立保留個人資料期限的政策，當中需考慮不同資料的類型、儲存的媒體及保留資料的目的，並訂明如何辨識已超過保留期限的資料及銷毀有關資料的程序及方式。

(8) 恰當地使用個人資料

私隱專員注意到其中兩所機構在提供補習服務時涉及不恰當地使用個人資料。私營補習機構應全面檢討其使用個人資料的情況，以確保其使用個人資料的目的與當初收集資料的目的一致或直接有關，或已獲取資料當事人的訂明同意。

(9) 完善的個人資料保安制度

私隱專員發現該三所私營補習機構在不同的操作及系統中均涉及保安不足的情況。私營補習機構越來越倚重資訊科技系統處理補習相關服務、保存及管理有關記錄和資料庫。因

此，保持資訊科技系統的健康運作以避免系統受網絡攻擊，與其他實體保安措施同樣重要。

(i) 制定實體保安措施，例如出入系統、將重要文件上鎖等，以避免或防止未獲授權人士查閱及使用個人資料；
(ii) 利用加密程式、系統登入管理、身份認證管理等措施以限制及監控在資訊科技系統中查閱及存取個人資料的情況；及
(iii) 制定全面的資訊保安政策，輔以定期的培訓，以加強員工對個人資料私隱的意識。

(10) 以合約方式管理資料處理者

私隱專員滿意該三所機構在聘任資料處理者在處理個人資料時，以合約方式規範資料處理者有關個人資料的保留及保安事宜。私營補習機構除應以合約方式規範資料處理者在處理其委託的個人資料的情況外，亦應定期進行適當的監控及審查程序，以確保資料處理者符合有關私隱保障的要求。

在與大型雲端服務供應商購買雲端服務時，私營補習機構應小心評估供應商可靠程度、該服務的內容，以及標準合約內的條款及細則是否符合所有資料保障的要求。

作為良好的行事方式，機構應進行詳細的私隱影響評估，在向供應商託付個人資料前辨識潛在的私隱風險。

(11) 資料倫理道德標準

由於機構能從個人資料獲取利益，因此在營運上不應抱有只依從最低監管要求的想法。機構應恪守更高的道德標準，以在實際營運上符合持份者的期望。數據道德的概念可彌補法例要求和持份者期望兩者之間的落差。

– 完 –

香港私營補習服務行業的個人資料系統

視察報告

(I) 簡介

視察原因

1. 香港，如同中國大陸、日本及台灣等其他亞洲主要法域區，非常著重學童的學業成績及公開考試成績。因此，私營補習服務百花齊放，私營補習學校的大型廣告比比皆是，成為學童在傳統學校外獲得學業知識的主要渠道。根據調查資料顯示，超過 76%學童曾接受私營補習服務，當中 22%學童早於小學四年級起已經開始接受這類輔導教育。

2. 香港現時有超過 2,000 所私營補習機構，主要服務對象為中小學生。由於學童傾向毫不猶豫地依從指示、私隱意識偏低，因此他們在接受這類私營補習服務時應特別給予私隱保障。此外，私營補習機構在提供相關服務時，亦會收集及處理學童家長及補習導師的個人資料。他們收集及處理的個人資料數目非常龐大，當中不乏較為敏感的個人資料（例如香港身份證（身份證）號碼），私隱專員認為根據《個人資料（私隱）條例》（條例）第 36 條對私營補習機構的個人資料系統進行視察，符合公眾利益。

(II) 視察

<u>私營補習服務行業</u>

3. 香港的私營補習服務種類繁多，由獨立運作的私營補習中心，以至連鎖式的私營補習機構；由傳統透過導師面授課程內容，以至利用錄影影像或網上媒體作教學工具，各適其適。

4. 私隱專員從以下的私營補習服務形式中各挑選了一所具代表性的機構作為視察對象，以了解私營補習服務市場的資料使用者就收集、持有、處理及使用個人資料方面的運作：

(i) 連鎖式經營的補習機構；
(ii) 以特許經營模式營運的補習機構；及
(iii) 利用網上媒體（網頁及流動應用程式）提供補習服務的機構。

連鎖式私營補習機構

5. 連鎖式私營補習機構運營多個補習中心，有著大量的學童人數與傳統教育人數相約。除了由補習導師在課堂面授的模式外，現亦發展出以錄影影像授課的課程或透過網上媒體的自學課程。私隱專員挑選了一所市場佔有率頗高，在全港不同的地區設有分校的補習機構A（**機構 A**）作為本視察的對象。機構 A 每年的課程報讀人數超過60,000 人次。

特許經營模式營運的私營補習機構

6. 利用特許經營模式營運的私營補習機構在香港亦很普遍。這類型的補習機構的特點是擁有大量補習中心，每班學童數量相對較少。有意營運該補習機構品牌的人士可申請以特許經營模式加盟。雖然所有補習中心均以同一品牌營運，但該補習機構及個別特許經營的補習中心屬不同的法人團體，就個人資料私隱而言，他們可被視為聯合的資料使用者。特許經營人士會接受統一的教學工具、營運培訓及支援。私隱專員挑選在全港建立了多所補習中心的補習機構 B（**機構 B**）為本視察的其一對象。

利用網上媒體提供補習服務的機構

7. 機構 C（**機構 C**）建構了一個流動應用程式，吸納學童及補習導師，並透過該程式作為網上補習平台，利用資訊科技工具配對學童及補習導師以解答學童提出的學業問題。他們亦有採用機器學習等工具完善其提供配對服務。

視察的範圍

8. 視察小組檢視了以上三所私營補習機構從收集至銷毀顧客（包括學童及其家長）[3]及補習導師的個人資料的整個流程，了解他們在處理及保障個人資料方面的強弱之處，並仔細研究及分析登記補習服務及聘任補習導師時的個人資料流程，從而作出建議，以協助私營補習機構遵從條例附表 1 的保障資料第 1 至 6 原則的規定。

9. 保障資料第 1 至 6 原則涵蓋個人資料的收集、準確性、保留期間、使用、保安、公開政策及查閱等方面。本視察亦就該三所機構在直接促銷活動中使用顧客的個人資料方面，檢視其依從條例第 6A 部相關條文的情況。除私隱條例條文的規定外，視察小組亦以私隱專員提倡的「私隱管理系統」為保障個人資料私隱的最佳行事方式作參考，以評估這三所機構在企業管治層面上保護私隱的情況。

10. 該 6 項保障資料原則、條例第 35B 至 35H 條有關在直接促銷中使用個人資料的條文，及私隱管理系統的簡表分別載列於附件 1 至 3，以供參考。

視察的方法

11. 本視察包括 5 項主要檢視工作：

a) 神秘到訪

12. 視察小組曾以神秘顧客的形式到訪機構 A 及 B 的補習中心，以全面了解報讀至提供補習課程的流程及補習中心員工的個別表現，尤其是他們在日常工作中處理個人資料的方式。由於機構 C 是透過流

[3] 在本視察中，學童資料經常性包含其家長的個人資料，尤其當考慮到學童的年齡尚小。因此，為簡化文字的目的，在本文以後的「學童資料」（或類似字眼）已包括學童及其家長的個人資料。

動應用程式提供補習服務，視察小組則以用家身分登記及測試該應用程式，以了解其服務的流程。

b) 審閱政策

13. 一份詳細而全面的處理個人資料政策可確保員工的行事方式穩妥及一致。視察小組審閱了該三所機構就保障個人資料私隱制定的相關政策、指引、通告、表格和培訓資料。

c) 現場視察

14. 視察小組現場視察了該三所機構的總部，並揀選了機構 A 及 B 的部分補習中心及貨倉進行現場視察藉以（i）親身了解該三所機構收集、處理及儲存顧客個人資料的場所及相關保安措施；（ii）檢視用作收集、處理及儲存顧客個人資料的設備和系統；（iii）檢視場所和電腦系統內儲存的紙張記錄及電子記錄；及（iv）檢視其日常運作有否涉及不恰當處理個人資料的情況。

d) 示範

15. 在現場視察期間，該三所機構向視察小組示範了處理課程及相關服務的申請流程、顧客查詢等程序，讓視察小組了解他們如何收集、使用及保障個人資料。

e) 面談及查詢

16. 視察小組曾分別在進行本視察之前、過程中及之後，向該三所機構作口頭及書面查詢。視察小組透過面談向該三所機構總部及分行的職員，包括管理層及前線職員，作出口頭查詢，以了解他們處理個人資料的情況、對有關個人資料私隱的內部政策及指引的熟悉程度，以及他們所提供和接受的培訓資訊。視察小組亦與機構 C 位於台灣的技術部門進行視像會議，以了解他們保護其該程式的技術工具及方式。

17. 視察小組透過向該三所機構作出書面查詢，了解他們的個人資料系統的運作，把所取得的書面證明與現場視察所得的資料作出核對，及識別當中需要關注的事項。

(III) 個人資料系統及資料流程

個人資料系統

18. 本視察中審視的個人資料系統不但涵蓋用作處理個人資料的電腦系統，亦包括不同部門及相關補習中心在收集、持有、處理或使用學童及補習導師個人資料的系統運作。

19. 該三所私營補習機構的個人資料系統略所不同：

(i) 機構 A – 擁有數個電腦系統處理學童註冊、課程資訊及課程出席及調配等安排，其中央註冊系統負責記錄及處理學童在補習中心註冊課程的情況；
(ii) 機構 B – 特許經營補習中心會利用統一的課程申請表格收集學童的個人資料，而機構 B 的總部在接獲有關表格後會將資料輸入其電腦系統；
(iii) 機構 C – 透過流動應用程式收集學童及導師的個人資料，有關資料會直接傳送到其資料庫作進一步處理。

20. 該三所機構的個人資料系統內就課程登記所收集的學童及家長的個人資料[4]種類載列如下：

個人資料種類	**機構 A**	**機構 B**	**機構 C**
(1) 中英文姓名	√	√	
(2) 性別	√	√	
(3) 國籍		√	
(4) 身份證號碼	√		
(5) 出生日期	√	√	
(6) 年級	√	√	
(7) 聯絡電話號碼	√	√	√
(8) 電郵地址	√	√	√
(9) 社交媒體帳戶	√		

[4] 雖然有關的課程申請表格沒有訂明所要求的個人資料是否必須提供，但機構 A 及 B 均表示部份資料屬可選擇提供。

(10) 地址	√	√	
(11) 家長／監護人姓名	√	√	
(12) 與家長／監護人關係	√		
(13) 家長／監護人聯絡電話號碼	√	√	
(14) 家長／監護人電郵地址		√	
(15) 學校名稱	√	√	√

表一

21. 除姓名及聯絡資料外，該三所機構的個人資料系統內所涉及補習導師的其他個人資料種類載列如下：

個人資料種類	**機構 A**	**機構 B**	**機構 C**
(1) 身份證號碼	√	√	
(2) 身份證副本	√	√	
(3) 婚姻狀態	√	√	
(4) 出生日期	√	√	
(5) 學歷背景	√	√	
(6) 工作履歷	√	√	
(7) 專業資格	√	√	
(8) 推薦人姓名及聯絡資料	√	√	
(9) 緊急聯絡人姓名及聯絡資料	√	√	
(10) 銀行戶口號碼	√		√
(11) 性罪行定罪紀錄	√		
(12) 社交媒體帳戶			√
(13) 公開考試成績副本			√
(14) 大學學生證副本			√

表二

個人資料流程概覽

a) 機構 A

i) 收集個人資料

22. 機構 A 於各補習中心處理學童報讀課程註冊事宜。學童的個人資料流程由學童遞交課程申請表格開始，當中涉及收集上述表一所列載的個人資料。其後，補習中心職員會將表格上的資料輸入中央註冊系統，並列印課程收據。

23. 就補習導師的個人資料流程而言，機構 A 會透公司網頁收集求職者的招聘申請，當中會要求求職者提供姓名、聯絡資料及學歷及工作經驗等個人資料。機構 A 會邀請合適的求職者進行面試，並要求他們填寫求職表格，當中包括收集上述表二所列載的個人資料。

ii) 使用個人資料

24. 機構 A 在提供補習服務及處理內部行政事宜時會使用學童的個人資料作以下用途：

- 課程出席記錄；
- 就課堂特別安排聯絡學童；
- 於緊急情況聯絡學童家長；
- 處理學童的查詢及要求；
- 處理及核對交易記錄；及
- 提供市場推廣資訊。

25. 補習導師的個人資料主要用於招聘過程及人事管理的目的。

iii) 個人資料的保留

紙張記錄

26. 補習中心會將收集得的課程申請表格存放於受限制區域。其後，表格會傳送至總部與中央註冊系統作核對。完成核對後，表格會再運送至貨倉存檔，儲存期限為 10 年。
27. 在提供補習服務、處理內部行政事宜及作市場推廣活動時，機構 A 的總部及各補習中心均可從電腦系統中列印載有學童個人資料的報

告、聯絡名單及其他相關記錄。這些文件的保存期限由一天至七年不等。機構 A 有為部份文件制定政策，訂明相關的保留期限。

28. 所有補習導師的個人資料文件均存放於人事部位於總部的一個上鎖房間。不成功的求職者的個人資料會保存四個月，而前僱員的個人資料則會保存三年。所有在職員工的人事檔案均存放於上鎖櫃內，查閱有關資料須於人事部主管持有的記錄冊內登記。

電腦檔案

29. 除中央註冊系統以記錄及處理學童資料外，機構 A 亦管有一套出席記錄系統以處理學童出席課堂記錄、行政系統以記錄及處理學童提出的要求。該兩個系統連接中央註冊系統以獲取學童資料。此外，不同部門亦會因應工作需要自行編製載有學童個人資料的檔案。

30. 雖然機構 A 沒有制定相關的保留政策以訂明中央註冊系統及個別員工持有的電腦檔案的保存期限，但根據公司的常規，中央註冊系統內的學童資料如超過七年沒有活動，他們便會銷毀有關資料。中央註冊系統的備份會在加密後儲存於雲端服務。

31. 機構 A 沒有特定的電腦系統儲存及管理補習導師的資料。

32. 機構 A 所持有不同的載有個人資料的紙張文件及電腦檔案的保存期限表列如下：

檔案種類	**保留期限**
課程申請表格	10 年
報告、聯絡名單及其他相關載有學童資料的文件	1 日至 7 年
不成功的求職者資料	4 個月
前僱員的資料	3 年
沒有活動記錄的學童檔案	7 年

iv) *銷毀個人資料*

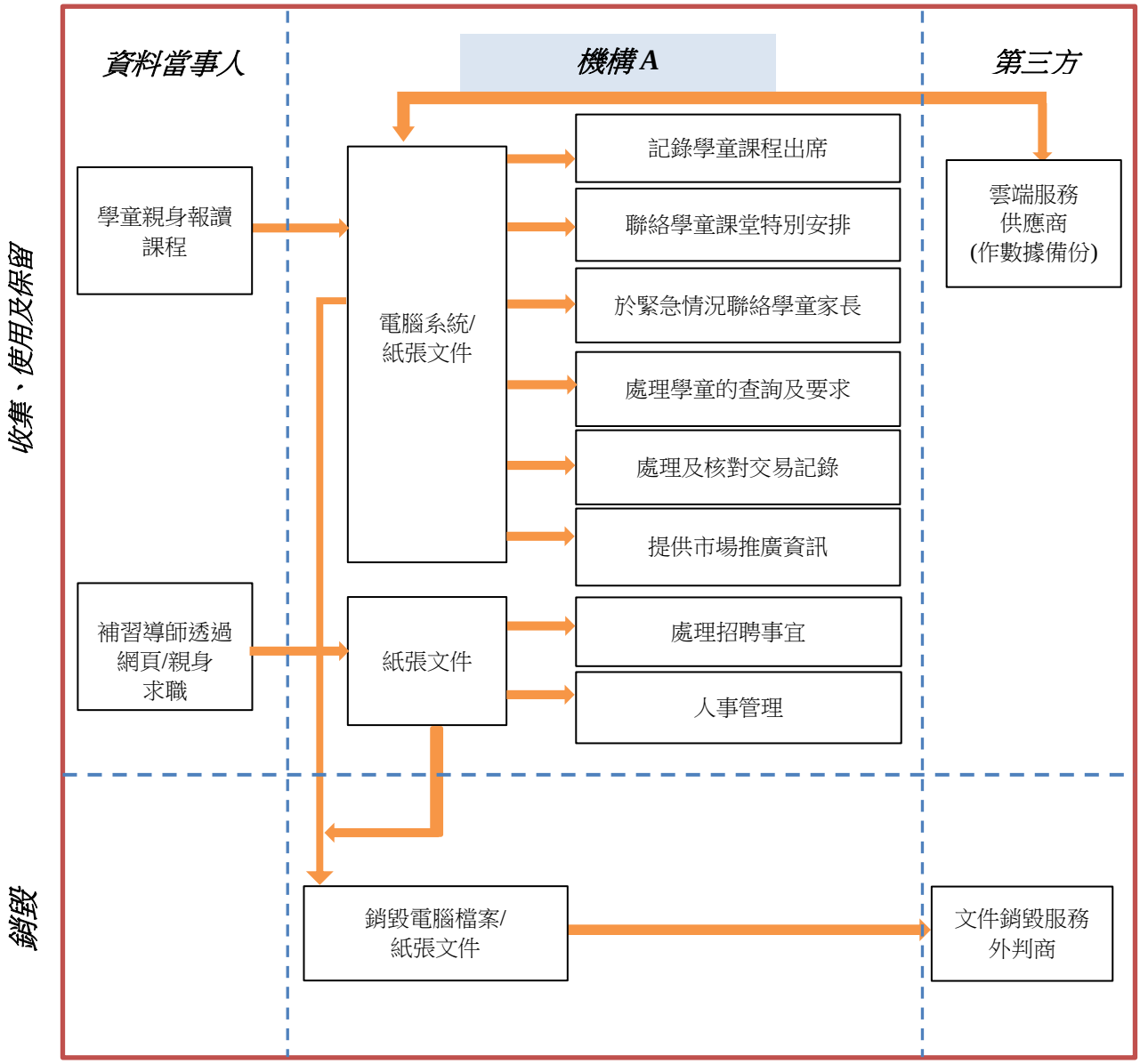
紙張記錄

33. 根據公司的慣常做法，當部門沒有足夠位置存放學童的記錄及文件時，他們會將有關文件運送至貨倉儲存。被存倉的文件均會記錄日期及文件種類。倉務員會根據文件日期及文件種類可保留的期限而將有關文件運送至指定的文件銷毀服務外判商以作銷毀。沒有運送至貨倉的文件則由部門自行切碎銷毀。

電腦檔案

34. 機構 A 沒有制定清除載有學童個人資料檔案的政策。根據公司的常規，中央註冊系統內的資料如超過七年沒有活動，資訊科技部便會銷毀有關資料。而儲存在個別員工的工作檔案則倚靠員工自行刪除。

35. 機構 A 的學童及補習導師的個人資料的流程簡述如下：



b) 機構 B

i) 收集個人資料

36. 特許經營的補習中心由個別特許經營人士自行經營。他們利用機構 B 提供的統一的課程申請表格收集學童的個人資料，當中涉及收集上述表一所列載的個人資料。課程申請表格一式三份，家長及補習中心各持有一份副本，另一份副本則會運送至總部，總部員工會將表格上的資料輸入電腦系統。

37. 如有意申請加盟並開設特許經營補習中心的人士，需於機構 B 的網頁提供初步個人資料，並參加其舉辦的特許經營介紹講座。在講座中，機構 B 會要求有意營運特許經營補習中心的人士填寫申請表格，並收集申請人的姓名、聯絡資料，以及上述表二所列載的個人資料。

ii) 使用個人資料

38. 機構 B 及其特許經營的補習中心在提供補習服務及處理內部行政事宜時會使用學童的個人資料作以下用途：

- 處理課程註冊及相關事宜；
- 給予優異學習進度獎勵；
- 聯絡學童家長；
- 進行內部統計及分析；
- 處理學童或其家長要求調配至其他補習中心或停讀後重新上課要求的事宜；及
- 提供產品、服務及活動的推廣資訊。

39. 特許經營人士的個人資料主要用於建立特許經營的補習中心、處理特許經營合約及監控補習導師的教學質素等事宜。

iii) 個人資料的保留

紙張記錄

40. 除課程申請表格外，學童會獲提供一本手冊，當中記錄學童的基本個人資料包括姓名、聯絡電話號碼、相片及學習進度等資料。手冊存放於補習中心，以記錄學童的學習進度。此外，機構 B 的總部亦

會於每月編制一份導師報告，當中顯示學童就讀的每個學科的進度資料。總部及個別補習中心均會持有課程申請表格及導師報告副本。

41. 在補習中心，手冊放置於當眼位置以便學童在上課時存取。同樣地，到訪者亦能輕易查閱及存取手冊內容。一般而言，個別補習中心會保留課程申請表格及前學童的手冊三至六個月，但導師報告的保留期限則個別補習中心都不盡相同。在總部，課程申請表格及導師報告則會存於上鎖櫃內，並分別保留四及六個月。

42. 特許經營人士的申請表格及相關合約會存放於總部的上鎖櫃內；而未能成功申請特許經營的人士及已終止特許經營合約人士的資料文件會保留六個月。

電腦檔案

43. 在視察過程中，視察小組注意到個別補習中心較少使用電腦處理學童資料。機構 B 使用不同的電腦系統分別處理及儲存學童及特許經營人士的資料檔案，而未能成功申請特許經營的人士及已終止特許經營合約人士的資料文件會則保留六個月，機構 B 沒有就保留學童及特許經營人士的資料檔案制定保留期限。

44. 機構 B 及特許經營補習中心所持有各類載有個人資料的紙張文件及電腦檔案的保存期限表列如下：

檔案種類	**資料保留者**	**保留期限**
課程申請表格	機構 B	4 個月
	補習中心	3 至 6 個月
前學童的手冊	補習中心	3 至 6 個月
導師報告	機構 B	6 個月
	補習中心	不定
未能成功申請特許經營及已終止特許經營合約人士的申請表及合約	機構 B	6 個月
未能成功申請特許經營人士的電腦檔案	機構 B	6 個月

學童的電腦檔案	機構 B	永久保留
已終止特許經營合約人士的電腦檔案	機構 B	永久保留

(iv) 銷毀個人資料

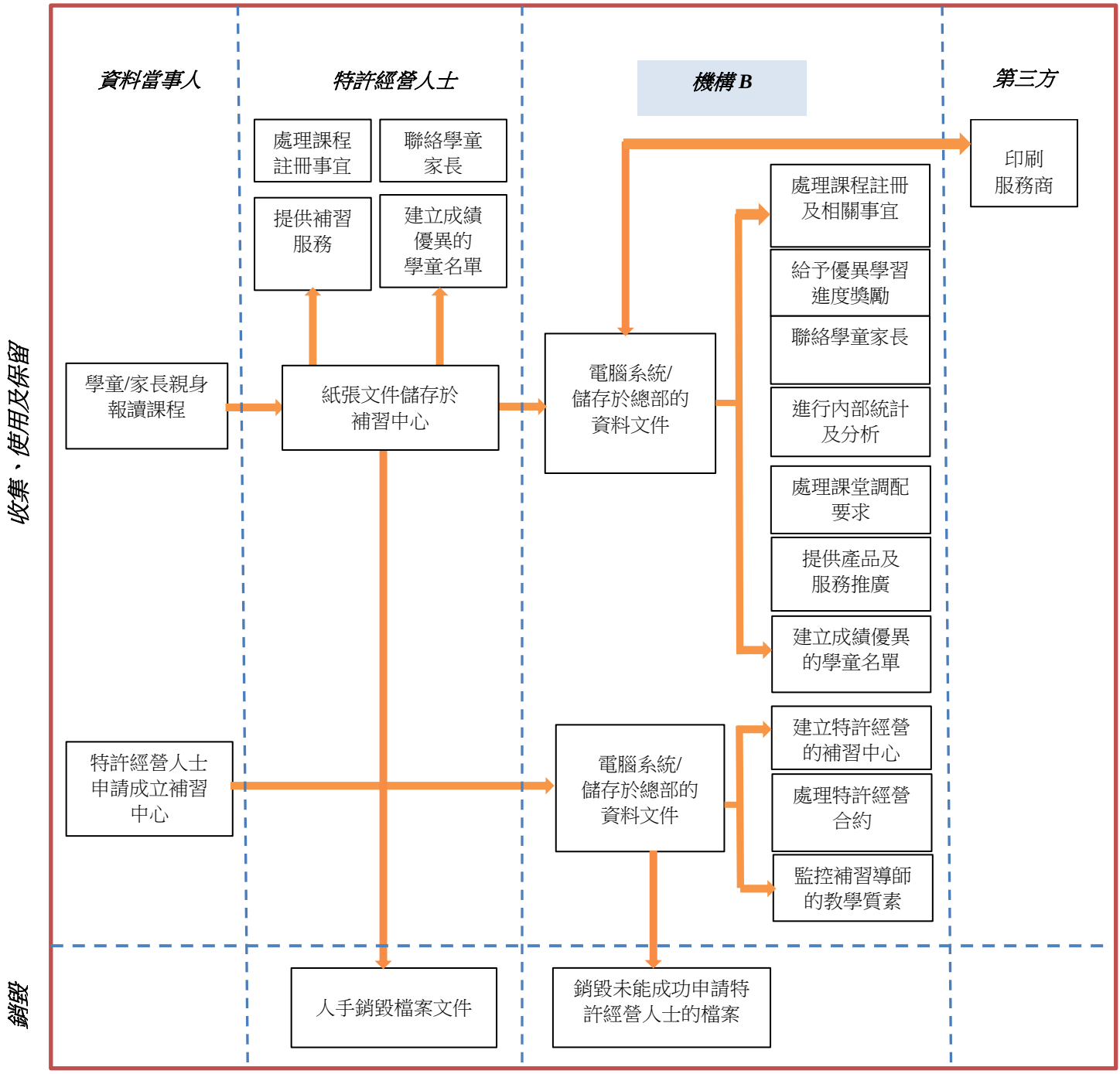
紙張記錄

45. 特許經營補習中心會人手銷毀已過保留期限的學童檔案文件；儲存於總部的學童檔案文件及特許經營人士的資料，機構 B 則會在特定房間以碎紙機銷毀。

電腦檔案

46. 由於個別特許經營補習中心較少使用電腦處理學童資料，視察小組未有發現相關的電腦檔案或記錄。然而，機構 B 除了會銷毀未能成功申請特許經營人士的檔案外，未有制定政策以銷毀或刪除載有個人資料的電腦檔案。

47. 機構 B 的學童及特許經營人士的個人資料的流程簡述如下：



c) 機構 C

i) 收集個人資料

48. 當學童及補習導師在機構 C 的流動應用程式登記成為用戶時，機構 C 便透過該程式收集他們的個人資料，當中涉及收集上述表一及表二所列載的個人資料。

ii) 使用個人資料

49. 學童在登入該程式後可在程式內發問學術問題；導師在登入該程式後可選擇解答已發問的問題。在發問及解答的過程中不涉及披露或使用個人資料。然而，機構 C 會利用機器學習等工具以配對導師解答符合其資歷及程度的問題。

50. 在試用期結束後，學童需要購買不同價值組合的補習服務才能繼續在該程式中發問。付款過程是透過第三方的付款平台處理，機構 C 不會收集及使用學童提供的信用卡資料， 但會將報酬給予導師提供的指定銀行戶口。

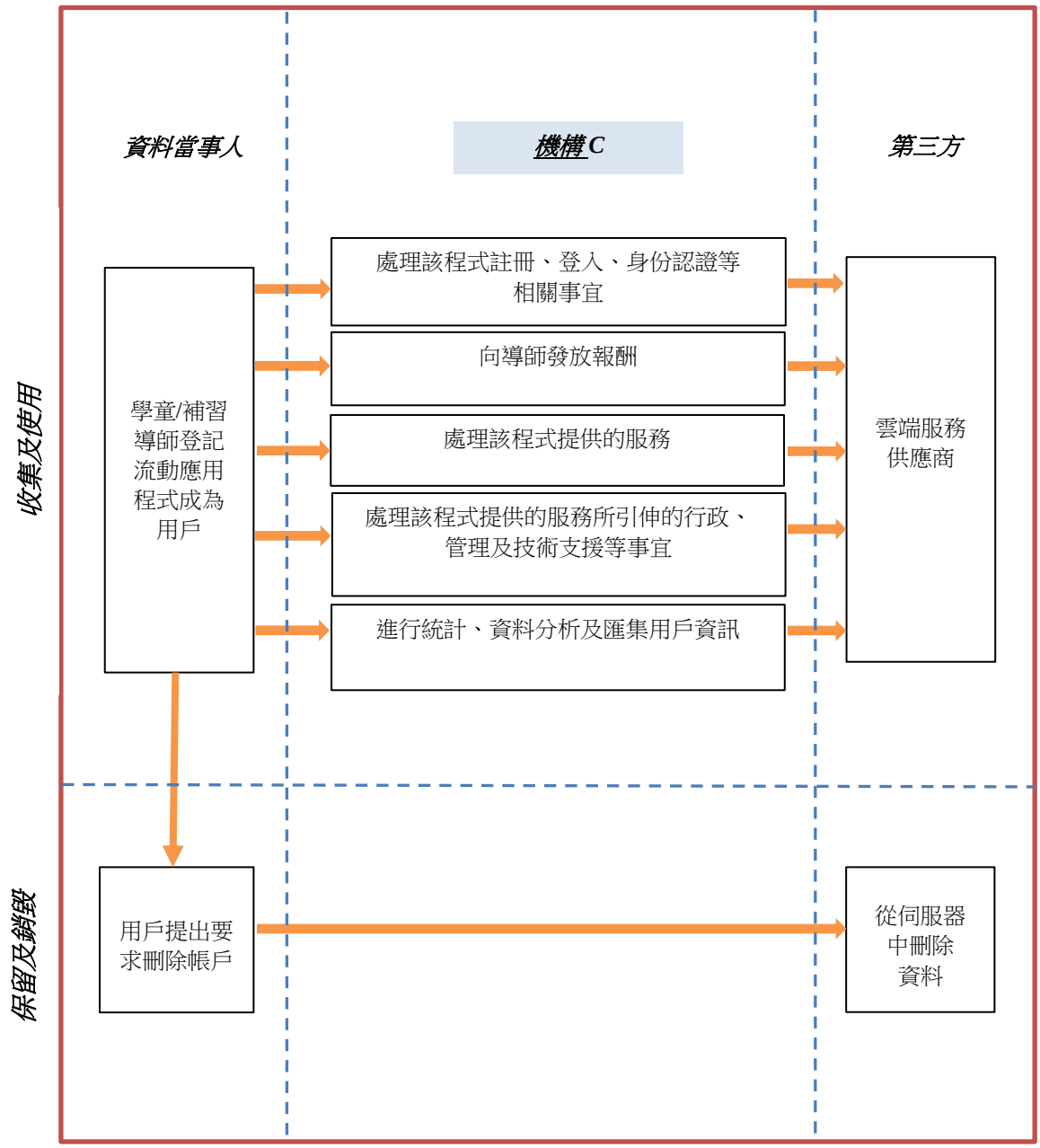
51. 機構 C 會使用收集得的個人資料作以下用途：

- 處理該程式註冊、登入、身份認證等相關事宜；
- 處理該程式提供的服務；
- 處理該程式提供的服務所引伸的行政、管理及技術支援等事宜；
- 向導師發放報酬；及
- 進行統計、資料分析及匯集用戶資訊。

iii) 保留及銷毀個人資料

52. 機構 C 沒有持有實體個人資料文件，所有資料均以電腦檔案形式儲存。該程式用戶的個人資料儲存於由第三方雲端服務供應商提供的外置伺服器內。用戶資料只會因應用戶作出的要求而刪除。

53. 機構 C 的學童及補習導師的個人資料的流程簡述如下：



(IV) 視察結果及建議

導言

54. 私隱專員根據該三所私營補習機構於本視察時所提供的資料及視察小組的實地觀察，得出視察結果及作出建議。有關結果及建議只反映在本視察時所見的循規情況，並不應被視為已全面涵蓋該三所機構的個人資料系統於各方面的運作。

55. 在整個視察過程中，私隱專員欣賞該三所機構均視學童及補習導師的個人資料為重要的資產，以不會胡亂處理或濫用的原則，致力確保他們的資料得到妥善管理。然而，機構的不同營商模式對私隱保障的理念有所不同，導致所採取的私隱保障措施方針有異。以流動應用程式作為提供補習服務平台的機構，能靠著本身擁有資訊科技技術的優勢，審慎地利用資訊科技工具分割及監控其電腦系統的存取權限，以減少未獲授權查閱或洩露個人資料的風險。私隱專員尤其欣賞該機構有效利用資訊科技工具，以顧客為本，將私隱保障納入其產品及服務設計之中，降低私隱外洩的風險。

56. 私隱專員注意到該三所機構在實際的營運過程及常規中，均有採取保障個人資料的措施。然而，有關措施只能零碎地從機構的個別職能中體現，而未有將私隱保障納入其企業管治之中。私隱專員認為，負責任的機構的最佳行事方式是建立及全面執行「私隱管理系統」。

執行「私隱管理系統」以保障個人資料私隱

57. 「私隱管理系統」的框架主要為將個人資料私隱保障納入企業管治責任，並在機構中貫徹執行，涵蓋業務常規、操作程序、產品及服務設計、實體建築，以至網絡基礎設施，並輔以適當的檢討及監察程序。整個系統必需是跨部門及跨職能，所有員工均應知悉及瞭解系統的運作，藉以配合機構遵從條例的規定。

a) 將私隱保障納入企業管治

	機構 **A**	機構 **B**	機構 **C**
營商模式	連鎖式	特許經營	網上平台
職員	約 300 人	約 200 人	約 15 人

學童/導師人數	學童約 279,000 人 導師 70 人	學童約 30,000 人 導師 150 人	學童約 103,000 人 導師 9,000 人
資料保障主任	沒有	副總經理	營運經理

58. 由管理層擔任資料保障主任可協助機構有效地管理及執行個人資料保障的政策，尤其是該三所機構均需處理大量學童（及導師）的個人資料。機構 B 及 C 均有委派一名管理層職員負責監督私隱事宜是值得欣賞的，私隱專員尤其欣賞機構 C 即使屬初創企業，亦正面地對私隱保障作出機構性的承諾。無論機構大小，私隱專員強烈鼓勵其他私營補習機構作出同樣的企業承擔。

建議

1. 私隱專員強烈鼓勵所有私營補習機構（不論其營商模式或機構大小）應將個人資料私隱保障納入企業管治，對此作出機構性的承諾；從最高管理層中委任保障資料主任，以管理私隱管理系統及資料保障相關事務，並在機構建立專重私隱的文化。

b) 貫徹私隱的設計

59. 私營補習機構因應香港教育需求的轉變及為提高其市場競爭力，不斷設計新的服務及推銷策略。從保障個人資料私隱的角度而言，機構應採取「貫徹私隱的設計」，在服務開發或設計時就將私隱保護的政策納入設計藍本，確保以用戶為中心，並依據服務類型定義出對應的隱私資料類型、處理方法及風險控制程序。

60. 在視察過程中，私隱專員發現不同的營商模式對不同的私營補習機構存有不同的影響。機構 C 的服務平台為流動應用程式，主要倚重資訊科技及網絡工具設計及運作其服務，他們在設計新產品或服務時已直接有效地利用資訊科技工具，以顧客為本，將私隱保障納入其產品及服務設計之中，降低私隱外洩的風險。另一方面，機構 A 在設計營銷活動時未有詳細考慮實際需要，在服務登記表格中收集學童的社交媒體帳戶，但卻沒有實質用途，亦沒有作出檢討以修訂表格，導致涉及收集不必要或過量的個人資料。

建議

2. 私營補習機構在設計新產品及服務時，應寓私隱保護於設計之中，並評估推出新產品及服務對個人資料私隱的影響。機構可有效利用資訊科技工具，以顧客為本，將私隱外洩風險降低。

c) 制定全面的私隱政策及資訊保安政策

61. 不論營商模式或機構規模，一份完備及詳細的私隱政策可協助私營補習機構推行及管理其不同部門及職能就收集、持有、處理、保護、銷毀及查閱個人資料等各方面的操作環節，並可因應其運作或服務的轉變而作定期檢討及更新有關政策。

	機構 **A**	機構 **B**	機構 **C**
營商模式	連鎖式	特許經營	網上平台
有否制定私隱政策或相關指引	有限度	只供總部參閱	沒有
有否制定資訊保安政策	有限度	沒有	只供位於台灣的技術人員參閱

62. 從本視察所得的資料，私隱專員認為該三所機構皆沒有全面的機構性私隱政策，私隱管理只能零碎地從機構的個別職能中體現，而未有納入企業管治中由上至下推行私隱政策。

63. 機構 A 委派人力資源部門負責發放企業指令予員工。例如，人力資源部門曾分別於 2016 及 2017 年向員工發出電郵，提醒他們有關正確使用外置儲存媒體及電腦保安的事宜，以避免個人資料外洩及網絡攻擊的風險。私隱專員認為這些措施毫無疑問能提升員工對個人資料私隱的認知，但私隱政策的制定應更為全面，並應持續定時傳閱有關政策。

64. 此外，機構 A 備有一份「內部管控程序手冊」[5]，以訂立及管控其資訊科技系統的內部措施，當中包括登入、密碼管理、電腦系統的

[5] Internal Controls Procedure Manual

維護及保安。該手冊卻只供高級管理層透過內聯網參閱，而且該手冊內容亦未有全面覆蓋所有主要的資訊保安問題或處理個人資料的情況。

65. 儘管機構 B 於 2017 年制定了有關保護個人資料的內部指引，該內部指引只適用於總部的員工，而實際日常接觸學童個人資料的特許經營補習中心卻對該內部指引毫不知情。私隱專員認為機構的私隱政策應適用於整個機構，隸屬同一機構的分行或特許經營補習中心（或其他不同營業模式的分店）不應存有不同的私隱政策和做法。

66. 另外，視察小組留意到機構 B 的部分補習中心設有閉路電視以保障學童安全。然而，機構 B 沒有對安裝或使用閉路電視制定相關政策，亦未有對此情況作出管理。同時，機構 B 亦沒有就資訊保安事宜制定一套資訊保安政策。

67. 機構 C 強調他們在設計產品及營運過程中已將私隱風險納入考慮及系統設定之中（例如：在系統設定查閱及修改資料的權限），認為無需刻意重覆地制定一份私隱政策。雖則如此，他們仍然為台灣的技術人員制定資訊科技保安及查閱資料政策。私隱專員欣賞機構 C 寓私隱保護於產品設計及營運之中，但認為作為一個負責任的機構，不應將制定私隱政策一事視為重覆或不必要的工作，而應將已採取的私隱保護及資訊保安措施清晰地匯編於私隱政策之中，讓所有員工清楚瞭解及遵從。此舉不但有利機構發展，亦可確保員工能符合機構對私隱保障的要求。

建議

3. 不論營商模式或機構大小，私營補習機構應就其處理個人資料的措施制定全面的私隱政策。有關的私隱政策必須適用於所有部門及補習中心，亦必須適時通知所有員工有關規定，以確保機構對處理個人資料的制度及措施一致。為配合社會及業務發展，機構亦應定期檢討及更新其私隱政策。

   私隱政策應涵蓋個人資料（包括文件及電子記錄）收集、準確性、保存期限、使用、保安措施、銷毀程序，以及處理直接促銷活動及拒收訊息的要求及操作程序等各項範疇。

4. 由於現時處理補習服務非常倚重資訊科技，安全的資訊科技系統尤為重要。私營補習機構應就資訊科技保安制定相關政策，訂明機構所有採取的資訊科技保安措施及應對相關保安風險的實務政策。

d) 建立有效的匯報系統及資料外洩事故通報機制

	機構 **A**	機構 **B**	機構 **C**
營商模式	連鎖式	特許經營	網上平台
有否委派專人負責處理分行事宜	有	有	不適用
資料外洩事故通報機制	不足夠	不足夠	有

68. 私隱專員欣悉機構 A 及 B 均有委派專職部門及員工負責處理不同補習中心的行政事宜。在視察的過程中，補習中心清楚知道如何匯報資料外洩事故。同時，兩所機構亦有透過定時探訪，以監察補習中心遵守相關政策及規定的情況。

69. 雖則如此，該兩所機構卻沒有書面指引或程序，規管處理資料遺失或外洩的情況。私隱專員認為制定清晰詳細的書面指引及程序可迅速回應此等事故，並能採取適時的補救措施，避免嚴重損失，尤其是在現時的數碼世界，非常容易遭受網絡攻擊。因此，迅速回應資料外洩事故能減低事故所帶來的影響及損失。

70. 作為透過網上平台提供補習服務的機構 C 則對網絡攻擊的情況甚為瞭解，亦因此制定有一套應對資料外洩事故的程序及跟進措施。在面談的過程中，機構 C 的員工亦清晰瞭解有關程序的內容。

建議

5. 為應對處理個人資料私隱的各項事宜，私營補習機構應建立一套有效的匯報及監控系統，以能適當地回應處理個人資料時所帶來的問題，並確保員工遵從機構制定的私隱政策。

6. 私營補習機構應制定資料外洩事故的通報機制，訂明處理此等事故的流程（包括如何遏止資料外洩及減少損失的即時評估及補救措施），並委派指定管理層負責處理此等情況。

e) 透過培訓及教育提升員工對私隱保障的意識

71. 健全的私隱管理系統有賴機構員工的配合，他們須知悉其保障個人資料的責任，並付諸實行。一套沒有員工依從的私隱管理系統形同虛設。因此機構應經常提醒相關員工依從機構的政策及系統監控。

	機構 **A**	機構 **B**	機構 **C**
營商模式	連鎖式	特許經營	網上平台
有否提供個人資料私隱的培訓	只限新入職員工	只限總部員工及補習中心導師	只限新入職員工

72. 在本視察的過程中，私隱專員留意到機構 A 及 C 都只會向新入職員工提供有關個人資料私隱的培訓。此外，機構 C 傾向透過採用系統工具以限制員工獲取或查閱個人資料的情況，因此認為無需定期向員工提供相關培訓。

73. 機構 B 定期向總部員工及補習中心的特許經營人士提供有關處理個人資料的講座及工作坊。他們亦在定期的機構通訊中載列有關資料

保障的議題及教育資訊。然而，機構 B 對個別補習中心的溝通只限於特許經營人士，並依賴他們發放有關資訊予補習中心的其他員工。私隱專員認為如此的溝通及培訓方式不夠全面。

建議

7. 為建立員工對私隱保障的意識及機構的尊重私隱文化，私營補習機構應定期提供教育及培訓予所有員工（包括特許經營人士及其員工或其他營商模式旗下的員工）。個人資料保障的全面培訓及複修課程不限於專門培訓課程、電郵或機構通訊內的實用提醒，以至內聯網內提供相關的資訊內容等。

因應私隱條例條文及保障資料原則的視察結果及建議

74. 除透過企業管治建立專重私隱的文化及監控以符合條例的規定外，私隱專員在視察的過程中發現該三所私營補習機構在日常的運作過程中涉及違反條例及保障資料原則的規定，並提出如下建議。

a) 停止不必要或過量收集個人資料

	機構 **A**	機構 **B**	機構 **C**
營商模式	連鎖式	特許經營	網上平台
不必要或過量收集個人資料	有	有	沒有

75. 視察小組不約而同在檢視機構 A 及 B 的課程申請表格後，發現他們均涉及向學童收集過量的個人資料，包括整個的出生日期。

76. 為配合營銷活動，機構 A 在課程申請表格中要求學童提供其社交媒體的帳戶，但沒有述明收集目的或訂明有關資料是否屬「可選擇提供」。同時，機構 A 在課程申請表格沒有提供個人資料收集聲明或相關資訊以符合保障資料原則第 1(3)原則的規定。

77. 在提供獎學金予公開考試成績優異的學童時，機構 A 會要求收集學童的身份證副本；而在提供免費試堂時，他們亦會在網上登記表格要求收集學童的身份證號碼。單純為核實身份的目的而言，私隱專員認為如此收集學童的身份證號碼或副本是不必要的，機構 A 可有其他替代方法以達至相同目的。

78. 機構 C 提供的該程式的登記過程中只涉及收集學童的聯絡資料；而登記成為導師的申請則需提供其聯絡資料、大學學生證副本，以及公開考試成績副本（以確認他有能力足以任教有關學科）。然而，該流動應用程式不會收集他們的信用卡資料。私隱專員滿意機構 C 只收集最少限度的個人資料。

建議

8. 私營補習機構應檢視其收集個人資料的做法：

(i) 他們應停止收集不必要或過量個人資料，修訂相關表格並刪除或銷毀已收集的個人資料；
(ii) 他們應在登記或申請表格上提供個人資料收集聲明，以通知學童及其家長有關的收集目的及保障資料第 1(3)原則所訂明的其他情況；及
(iii) 他們應因應服務的性質，盡量減少收集個人資料的種類。

b) 避免永久保留個人資料

	機構 **A**	機構 **B**	機構 **C**
營商模式	連鎖式	特許經營	網上平台
永久保留個人資料	有	有	有

79. 私隱專員對該三所私營補習機構在不同情況下採取了永久保留學童或導師的個人資料的做法感到失望。

80. 機構 A 設有特定的電郵郵箱及社交媒體帳戶以處理公眾查詢。然而，所有查詢的內容（當中涉及個人資料）是有意永久地保留。

81. 視察小組亦在檢查機構 A 的員工電腦及網絡儲存裝置時，發現：

(i) 機構 A 沒有制定機制或監控措施以確保員工儲存在其電腦或網絡儲存裝置的學童資料會被適時銷毀；及
(ii) 其電子檔案（包括課程出席證明及成績證明等文件）會永久儲存於網絡儲存裝置中。

82. 機構 B 表示他們會永久保留已停讀的舊生資料及前補習中心導師的資料作內部用途。此外，視察小組亦發現部份補習中心會不必要地保留已停讀的舊生的課程申請表格。私隱專員認為如此長期保留舊生及前導師的個人資料是不合理的。

83. 機構 C 則沒有為保留個人資料訂立政策或期限。在檢查其資料庫及系統時，視察小組發現所有已停止活動的帳戶資料會一直保留在系統之中。然而，機構 C 表示如有帳戶持有人要求刪除其個人資料，他們則會應其要求在資料庫中刪除有關資料。

建議

9. 永久保留個人資料會違反條例第 26 條及資料保障第 2(2)原則。私營補習機構應訂立保留個人資料期限的政策，當中需考慮不同資料的類型、儲存的媒體及保留資料的目的，並訂明如何辨識已超過保留期限的資料及銷毀有關資料的程序及方式。

c) 恰當地使用個人資料

	機構 **A**	機構 **B**	機構 **C**
營商模式	連鎖式	特許經營	網上平台
不恰當地使用個人資料	有	有	沒有

84. 機構 A 會為緊急聯絡目的從中央註冊系統編印學童的電話名單，但該電話名單卻載有學童的身份證號碼。此外，他們亦會從行政系統編制課堂出席名單以協助登記臨時出席的學童，該名單亦載有學童的部份身份證號碼。私隱專員認為為聯絡或登記課堂出席的目的而使用學童的身份證號碼是不必要的。

85. 為宣傳目的，機構 B 的部份補習中心會自行將成績優異的學童資料（包括學童的姓名、所獲的成績及等級）張貼在補習中心，但卻沒有在事前取得學童或其家長的同意。

86. 視察小組在視察過程中未有發現機構 C 涉及不恰當使用個人資料的情況。

建議

10. 私營補習機構應全面檢討其使用個人資料的情況，以確保其使用個人資料的目的與當初收集資料的目的一致或直接有關，或已獲取資料當事人的訂明同意。

d) 完善的個人資料的保安制度

	機構 **A**	機構 **B**	機構 **C**
營商模式	連鎖式	特許經營	網上平台
個人資料保安程度	低	低	中等

87. 整體而言，該三所私營補習機構均有一定程度的內部監控及資料保安系統。然而，在本視察的過程中，視察小組在他們不同的操作及系統中發現保安不足的情況。

88. 機構 A 存有以下資料保安風險：

(i) 學童的身份證號碼被預設為網上服務的預設密碼；
(ii) 學童的資料（包括相片及身份證號碼）會在登記課程出席時於相關系統中顯示，然而有關電腦放置於公眾地方，資料有機會被他人意外地檢視；
(iii) 未有制定全面的資訊科技保安政策，以管理流動儲存裝置的使用、資料加密的要求，以及密碼管理等情況；
(iv) 普遍使用網絡儲存裝置但沒有制定中央管理機制；及
(v) 沒有系統用戶使用記錄及系統異常使用的匯報機制。

89. 機構 B 存有以下資料保安風險：

(i) 在資料傳送的過程中，沒有為載有學童學習進度及潛在加盟特許經營的申請人的檔案進行加密；
(ii) 學童的學習手冊存放於補習中心的公眾地方，進入補習中心的任何人士均能輕易獲取；
(iii) 未有制定全面的資訊科技保安政策；及
(iv) 有補習中心的導師將載有學童個人資料的文件自行帶回家中處理及銷毀。

90. 機構 C 存有以下資料保安風險：

(i) 在傳送透過 iOS 平台的流動應用程式收集得的個人資料時沒有適當的加密保護；及
(ii) 資料庫儲存於第三方供應商提供的雲端系統，並單純依賴該供應商提供的雲端保安措施。

建議

11. 私營補習機構越來越倚重資訊科技系統處理補習相關服務、保存及管理有關記錄和資料庫。因此，保持資訊科技系統的健康運作以避免系統受網絡攻擊，與其他實體保安措施同樣重要。他們應:

(i) 制定實體保安措施，例如出入系統、將重要文件上鎖等，以避免或防止未獲授權人士查閱及使用個人資料；
(ii) 利用加密程式、系統登入管理、身份認證管理等措施以限制及監控在資訊科技系統中查閱及存取個人資料的情況；及
(iii) 制定全面的資訊保安政策，輔以定期的培訓，以加強員工對個人資料私隱的意識。

e) 以合約方式管理資料處理者

	機構 **A**	機構 **B**	機構 **C**
營商模式	連鎖式	特許經營	網上平台
聘任資料處理者的種類	廢棄文件處理	印刷	雲端服務
以合約方式規範資料處理者	有	有	有

91. 私隱專員滿意該三所機構在聘任資料處理者在處理個人資料時，以合約方式規範資料處理者有關個人資料的保留及保安事宜。

建議

12. 私營補習機構除應以合約方式規範資料處理者在處理其委託的個人資料的情況外，亦應定期進行適當的監控及審查程序，以確保資料處理者符合有關私隱保障的要求。

13. 在與大型雲端服務供應商購買雲端服務時，私營補習機構應小心評估供應商可靠程度、該服務的內容，以及標準合約內的條款及細則是否符合所有資料保障的要求。作為良好的行事方式，機構在向雲端服務供應商託付個人資料前應進行詳細的私隱影響評估，以辨識潛在的私隱風險。

總結

92. 本視察已覆蓋本港主要營商模式的私營補習機構的個人資料系統及資料當事人由收集以至銷毀個人資料的生命週期。私隱專員留意到不同營商模式的補習機構對處理個人資料存有不同的理念及認知，導致他們的個人資料系統在不同方面各有長短。例如以科技為本的補習機構著重以系統工具限制存取個人資料的權限，以達至保障個人資料的目的。本視察的目的是讓整個私營補習市場了解同業良好的保護個人資料的行事方式，在行業中互相學習，取長補短，及完善自身的政策及運作常規，以遵守條例的規定，採用資料管治，建立「保障與尊重個人資料私隱」的文化。

93. 2018 年 5 月，歐盟發表了新的通用資料保護規則及嚴格要求，除其他外，資料控制者透過企業管治規範及保護其持有的個人資料。雖然香港現行未有類似法規，但將保障個人資料私隱納入企業管治的範籌絕對是全球趨勢。因此，私隱專員強烈提倡機構應採取「私隱管理系統」，詳情可從公署網站：https://www.pcpd.org.hk/pmp/guide.html 下載，以提升企業問責性，並與顧客建立互信的基礎，以期在處理私隱的過程達至雙贏。

94. 由於機構能從個人資料獲取利益，因此在營運上不應抱有只依從最低監管要求的想法。機構應恪守倫理更高的道德標準[6]，以在實際營運上符合持份者的期望。數據道德的概念可彌補法例要求和持份者期望兩者之間的落差。

95. 私隱專員鳴謝該三所私營補習機構及其員工的合作，令視察小組得以詳細了解其資料流程，以及其收集、保留和處理個人資料的原因。私隱專員尤其感謝他們為視察行動提供超越其職責範疇的協助。

– 完 –

[6] 公署於 2018 年 8 月員委託顧問公司進行「處理數據的正當性」研究項目，旨為探討機構如何透過提倡道德數據管治文化。該報告可從公署網站：https://www.pcpd.org.hk/misc/files/Ethical_Accountability_Framework.pdf 下載。

附件1 － 保障資料原則

1. 第1原則－收集個人資料的目的及方式

(1) 除非—

(a) 個人資料是為了直接與將會使用該資料的資料使用者的職能或活動有關的合法目的而收集；

(b) 在符合(c)段的規定下，資料的收集對該目的是必需的或直接與該目的有關的；及

(c) 就該目的而言，資料屬足夠但不超乎適度，

否則不得收集資料。

(2) 個人資料須以—

(a) 合法；及

(b) 在有關個案的所有情況下屬公平，

的方法收集。

(3) 凡從或將會從某人收集個人資料，而該人是資料當事人，須採取所有切實可行的步驟，以確保—

(a) 他在收集該資料之時或之前，以明確或暗喻方式而獲告知—

(i) 他有責任提供該資料抑或是可自願提供該資料；及

(ii) (如他有責任提供該資料)他若不提供該資料便會承受的後果；及

(b) 他—

(i) 在該資料被收集之時或之前，獲明確告知—

(A) 該資料將會用於甚麼目的(須一般地或具體地說明該等目的)；及

(B) 該資料可能移轉予甚麼類別的人；及

(ii) 在該資料首次用於它們被收集的目的之時或之前，獲明確告知—

(A) 他要求查閱該資料及要求改正該資料的權利；

(B) 處理向有關資料使用者提出的該等要求的個人的姓名(或職銜)及其地址，

但在以下情況屬例外：該資料是為了在本條例第8部中指明為個人資料就其而獲豁免而不受第6保障資料原則的條文所管限的目的而收集，而遵守本款條文相當可能會損害該目的。

2. 第2原則 — 個人資料的準確性及保留期間

(1) 須採取所有切實可行的步驟，以—

(a) 確保在顧及有關的個人資料被使用於或會被使用於的目的(包括任何直接有關的目的)下，該個人資料是準確的；

(b) 若有合理理由相信在顧及有關的個人資料被使用於或會被使用於的目的(包括任何直接有關的目的)下，該個人資料是不準確時，確保—

(i) 除非該等理由不再適用於該資料(不論是藉着更正該資料或其他方式)及在此之前，該資料不得使用於該目的；或

(ii) 該資料被刪除；

(c) 在於有關個案的整體情況下知悉以下事項屬切實可行時—

(i) 在指定日當日或之後向第三者披露的個人資料，在顧及該資料被使用於或會被使用於的目的(包括任何直接有關的目的)下，在要項上是不準確的；及

(ii) 該資料在如此披露時是不準確的，

確保第三者—

(A) 獲告知該資料是不準確的；及

(B) 獲提供所需詳情，以令他能在顧及該目的下更正該資料。

(2) 須採取所有切實可行的步驟，以確保個人資料的保存時間不超過將其保存以貫徹該資料被使用於或會被使用於的目的(包括任何直接有關的目的)所需的時間。

(3) 在不局限第(2)款的原則下，如資料使用者聘用(不論是在香港或香港以外聘用)資料處理者，以代該資料使用者處理個人資料，該資料使用者須採取合約規範方法或其他方法，以防止轉移予該資料處理者的個人資料的保存時間超過處理該資料所需的時間。

(4) 在第(3)款中—

資料處理者 (data processor) 指符合以下兩項說明的人—

(a) 代另一人處理個人資料；及

(b) 並不為該人本身目的而處理該資料。

3. 第3原則 — 個人資料的使用

(1) 如無有關的資料當事人的訂明同意，個人資料不得用於新目的。

(2) 資料當事人的有關人士可在以下條件獲符合的情況下，代該當事人給予為新目的而使用其個人資料所規定的訂明同意—

(a) 該資料當事人—

(i) 是未成年人；

(ii) 無能力處理本身的事務；或

(iii) 屬《精神健康條例》(第136章)第2條所指的精神上無行為能力；

(b) 該資料當事人無能力理解該新目的，亦無能力決定是否給予該項訂明同意；及

(c) 該有關人士有合理理由相信，為該新目的而使用該資料明顯是符合該資料當事人的利益。

(3) 即使資料使用者為新目的而使用資料當事人的個人資料一事，已得到根據第(2)款給予的訂明同意，除非該資料使用者有合理

理由相信，如此使用該資料明顯是符合該當事人的利益，否則該資料使用者不得如此使用該資料。

(4) 在本條中—

新目的 (new purpose) 就使用個人資料而言，指下列目的以外的任何目的—

(a) 在收集該資料時擬將該資料用於的目的；或

(b) 直接與(a)段提述的目的有關的目的。

4. 第4原則 — 個人資料的保安

(1) 須採取所有切實可行的步驟，以確保由資料使用者持有的個人資料(包括採用不能切實可行地予以查閱或處理的形式的資料)受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響，尤其須考慮—

(a) 該資料的種類及如該等事情發生便能做成的損害；

(b) 儲存該資料的地點；

(c) 儲存該資料的設備所包含(不論是藉自動化方法或其他方法)的保安措施；

(d) 為確保能查閱該資料的人的良好操守、審慎態度及辦事能力而採取的措施；及

(e) 為確保在保安良好的情況下傳送該資料而採取的措施。

(2) 在不局限第(1)款的原則下，如資料使用者聘用(不論是在香港或香港以外聘用)資料處理者，以代該資料使用者處理個人資料，該資料使用者須採取合約規範方法或其他方法，以防止轉移予該資料處理者作處理的個人資料未獲准許或意外地被查閱、處理、刪除、喪失或使用。

(3) 在第(2)款中—

資料處理者 (data processor) 具有第2保障資料原則第(4)款給予該詞的涵義。

5. 第5原則 — 資訊須在一般情況下可提供

須採取所有切實可行的步驟，以確保任何人—

(a) 能確定資料使用者在個人資料方面的政策及實務；

(b) 能獲告知資料使用者所持有的個人資料的種類；

(c) 能獲告知資料使用者持有的個人資料是為或將會為甚麼主要目的而使用的。

6. 第6原則 — 查閱個人資料

資料當事人有權—

(a) 確定資料使用者是否持有他屬其資料當事人的個人資料；

(b) 要求—

(i) 在合理時間內查閱；

(ii) 在支付並非超乎適度的費用(如有的話)下查閱；

(iii) 以合理方式查閱；及

(iv) 查閱採用清楚易明的形式的，

個人資料；

(c) 在(b)段所提述的要求被拒絕時獲提供理由；

(d) 反對(c)段所提述的拒絕；

(e) 要求改正個人資料；

(f) 在(e)段所提述的要求被拒絕時獲提供理由；及

(g) 反對(f)段所提述的拒絕。

附件 2 －在直接促銷中使用個人資料 （條例第 35B 至 35H 條）

35B － 適用範圍

本分部並不就要約提供以下服務或就有以下服務可予提供而進行廣告宣傳而適用—

(a) 由社會福利署營辦、資助或津貼的社會服務；

(b) 由醫院管理局或衞生署提供的醫護服務；或

(c) 符合以下說明的任何其他社會或醫護服務：該項服務擬向某名個人提供，而如不向該名個人提供該項服務，便相當可能會對以下人士的身體或精神健康造成嚴重損害—

(i) 該名個人；或

(ii) 任何其他個人。

35C － 資料使用者將個人資料用於直接促銷前，須採取指明行動

(1) 除第35D條另有規定外，資料使用者如擬在直接促銷中，使用某資料當事人的個人資料，須採取第(2)款指明的每一項行動。

(2) 資料使用者須—

(a) 告知有關資料當事人—

(i) 該資料使用者擬如此使用有關個人資料；及

(ii) 該資料使用者須收到該當事人對該擬進行的使用的同意，否則不得如此使用該資料；

(b) 向該當事人提供關於該擬進行的使用的以下資訊—

(i) 擬使用的個人資料的種類；及

(ii) 該資料擬就甚麼類別的促銷標的而使用；及

(c) 向該當事人提供一個途徑，讓該當事人可在無需向該資料使用者繳費的情況下，透過該途徑，傳達該當事人對上述的擬進行的使用的同意。

(3) 不論個人資料是否由有關資料使用者從有關資料當事人收集的，第(1)款均適用。

(4) 根據第(2)(a)及(b)款提供的資訊，須以易於理解的方式呈示，如屬書面資訊，則亦須以易於閱讀的方式呈示。

(5) 除第35D條另有規定外，資料使用者未經採取第(2)款指明的每一項行動，而在直接促銷中，使用某資料當事人的個人資料，即屬犯罪，一經定罪，可處罰款$500000及監禁3年。

(6) 在為第(5)款所訂罪行而提起的法律程序中，被控告的資料使用者如證明自己已採取所有合理預防措施，並已作出一切應作出的努力，以避免犯該罪行，即可以此作為免責辯護。

(7) 凡有法律程序為第(5)款所訂罪行而提起，在該程序之中，有關資料使用者負有舉證責任，證明由於第35D條，本條並不適用。

35D — 在何種情況下第35C條不適用

(1) 如在本部生效日期之前—

(a) 某資料當事人已獲某資料使用者以易於理解和(如以書面方式告知)閱讀的方式明確告知，其個人資料擬在或在直接促銷中，就某類別的促銷標的而被使用；

(b) 該資料使用者已如此使用該當事人的任何資料；

(c) 該當事人沒有要求該資料使用者停止如此使用該當事人的任何資料；及

(d) 該資料使用者沒有就該項使用而違反於該項使用時有效的本條例的任何條文，

而該資料使用者在本部生效日期當日或之後，擬在或在直接促銷中，就該類別的促銷標的而使用該當事人的不時更新的有關個人資料，則第35C條並不就該項擬進行的使用或使用而適用。

(2) 如—

(a) 某資料當事人的個人資料是由該當事人以外的另一人(***第三者***)提供予某資料使用者的；及

(b) 該第三者已書面通知該資料使用者—

(i) 就提供該資料而言，第35J及35K條已獲遵守；及

(ii) 該資料使用者可在直接促銷中，就何種類別的促銷標的(該當事人已同意者)使用該資料，

而該資料使用者擬在或在直接促銷中，就該類別的促銷標的而使用該資料，則第35C條並不就該項擬進行的使用或使用而適用。

(3) 在本條中—

本部生效日期 (commencement date) 指本部開始實施的日期；

有關個人資料 (relevant personal data) 就資料當事人而言，指該當事人的符合以下說明的個人資料：在緊接本部生效日期前，該資料的使用，受某資料使用者控制。

35E — 如無資料當事人同意，資料使用者不得將個人資料用於直接促銷

(1) 已遵守第35C條的資料使用者不得在直接促銷中，使用有關資料當事人的個人資料，但如以下條件獲符合，則不在此限—

(a) 該資料使用者已收到該當事人對擬如此使用(如該資料使用者根據第35C(2)(b)條提供的資訊所描述者)該個人資料的同意，不論是一般的同意或是選擇性的同意；

(b) (如該項同意屬口頭同意)該資料使用者已自收到該項同意起計的14日內，向該當事人發出確認以下事宜的書面確認—

(i) 收到該項同意的日期；

(ii) 有關許可種類個人資料；及

(iii) 有關許可類別促銷標的；及

(c) 該項使用符合該當事人的同意。

(2) 就第(1)(c)款而言，如—

(a) 有關個人資料屬某許可種類個人資料；及

(b) 該資料是就某促銷標的而使用，而該促銷標的屬某許可類別促銷標的，

則該項使用即屬符合該當事人的同意。

(3) 資料當事人可透過回應途徑或其他方法，向資料使用者傳達對使用個人資料的同意。

(4) 資料使用者違反第(1)款，即屬犯罪，一經定罪，可處罰款$500000及監禁3年。

(5) 在為第(4)款所訂罪行而提起的法律程序中，被控告的資料使用者如證明自己已採取所有合理預防措施，並已作出一切應作出的努力，以避免犯該罪行，即可以此作為免責辯護。

35F — 資料使用者首次將個人資料用於直接促銷時須通知資料當事人

(1) 在將某資料當事人的個人資料首次在直接促銷中使用時，資料使用者須告知該當事人，如該當事人要求該資料使用者停止在直接促銷中使用該資料，該資料使用者須在不向該當事人收費的情況下，停止在直接促銷中使用該資料。

(2) 不論個人資料是否由有關資料使用者從有關資料當事人收集的，第(1)款均適用。

(3) 資料使用者違反第(1)款，即屬犯罪，一經定罪，可處罰款$500000及監禁3年。

(4) 在為第(3)款所訂罪行而提起的法律程序中，被控告的資料使用者如證明自己已採取所有合理預防措施，並已作出一切應作出的努力，以避免犯該罪行，即可以此作為免責辯護。

35G — 資料當事人可要求資料使用者停止將個人資料用於直接促銷

(1) 資料當事人可隨時要求資料使用者停止在直接促銷中使用該當事人的個人資料。

(2) 不論有關資料當事人—

(a) 是否已自有關資料使用者，收到第35C(2)條規定須就使用有關個人資料提供的資訊；或

(b) 有否在較早前，向該資料使用者或第三者給予對該項使用的同意，

第(1)款均適用。

(3) 資料使用者如收到資料當事人根據第(1)款作出的要求，須在不向該當事人收費的情況下，依從該項要求。

(4) 資料使用者違反第(3)款，即屬犯罪，一經定罪，可處罰款$500000及監禁3年。

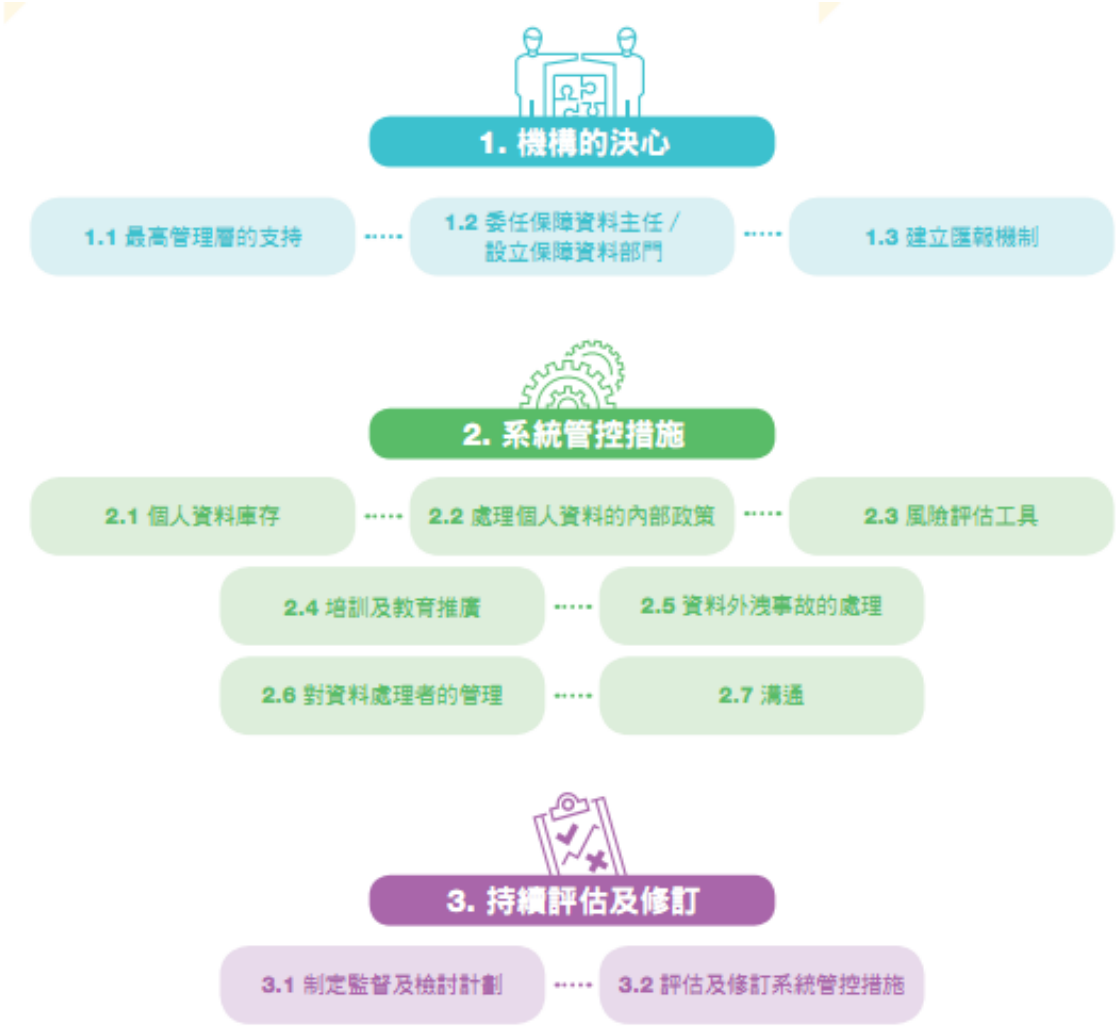
(5) 在為第(4)款所訂罪行而提起的法律程序中，被控告的資料使用者如證明自己已採取所有合理預防措施，並已作出一切應作出的努力，以避免犯該罪行，即可以此作為免責辯護。

(6) 本條不影響第26條的施行。

35H － 第3保障資料原則規定的對在直接促銷中使用個人資料的訂明同意

儘管有第 2(3)條的規定，凡根據第 3 保障資料原則，資料使用者在直接促銷中使用某資料當事人的任何個人資料，須獲該當事人的訂明同意，該資料使用者如沒有違反第 35C、35E 或 35G 條，即視為已取得該項同意。

附件 3 －私隱管理系統的摘要



— 本報告完 —