討論文件

二零二零年一月二十日

立法會政制事務委員會

《個人資料(私隱)條例》的檢討

目的

本文件就《個人資料(私隱)條例》(《私隱條例》)的檢討事宜徵詢委員意見。

《私隱條例》的檢討工作

2. 資訊和通訊科技發展一日千里，互聯網及流動通訊變得普及，科技的進步為個人資料私隱的保障帶來不少新挑戰。個人資料私隱違規事故的成因過往主要涉及不當收集和使用個人資料、直接行銷等，至近年則有轉為與數碼平台和資料保安相關的趨勢，當中包括個人資料外洩、保安系統出現漏洞以致受到黑客入侵、透過網上平台不當披露他人個人資料等問題。去年發生的一系列重大個人資料外洩事故，亦令公眾越來越關注《私隱條例》是否足以保障個人資料私隱。

3. 政府現正聯同個人資料私隱專員公署(公署)檢討並研究修訂《私隱條例》，以加強對個人資料的保障。

我們在檢討和研究修例方向的過程中參考了歐盟的《通用數據保障條例》及其他司法管轄區的經驗和相關法例，我們亦會留意各地尤其歐盟在加強私隱保障方面的發展趨勢，並考慮香港的實際情況，以期提出與時並進的修例建議。公署較早前已向政府作出修訂《私隱條例》的初步建議。我們目前集中研究的幾個修訂條例的方向列載於下文，歡迎委員就初步修例方向提出意見。

條例修訂建議

(I) 強制資料外洩通報機制

4. 《私隱條例》的第四項資料保障原則訂明，資料使用者須採取所有切實可行的步驟，保障個人資料不會未經授權或意外地被查閱。然而，現行法例並無規定資料使用者必須向公署或資料當事人通報資料外洩事故，目前有關通報是自願性質。引入強制通報機制規定資料使用者必須向公署和有關的資料當事人通報資料外洩事故，能確保私隱專員(專員)得以監察該等機構處理事故的做法，而該等機構亦可向專員尋求指示作跟進，以減低或防止其因事故而引致進一步損失。

5. 我們初步認為設立強制資料外洩通報機制應考慮以下幾點：

(a) 「個人資料外洩」的定義：指發生違反資料保安的情況而引致傳送、儲存或處理的

個人資料意外地或不法地被損毀、喪失、更改、未經授權而披露或被查閱[1]；

(b) 通報的門檻：資料外洩事故如「構成重大損害的真正風險」，資料使用者便應向公署及受影響人士通報。我們正研究資料使用者向上述兩者作出通報的門檻應否一樣，以及資料使用者決定有關資料外洩是否達到以上通報門檻時應考慮的因素，如外洩資料的種類和數量、資料的保安程度(例如外洩資料本身是否被加密處理)等；

(c) 通報的時限：資料使用者須在得知資料外洩後一段特定時間(例如於切實可行的情況下盡快通報，並在任何情況下不得多於五個工作天)內向公署通報資料外洩事故。公署亦應獲授權指示資料使用者向受影響人士通報。我們正研究是否有需要容許資料使用者於懷疑發生資料外洩事故時於既定時限內先進行調查並在期限內作出通報；以及

(d) 通報的方式：我們正研究容許資料使用者以電郵、傳真或郵遞方式向公署作出書面通報。而通報內容可包括資料保安事故的描述、資料外洩的原因、涉及的個人資料的種類和數量、危害風險評估、資料使用

[1] 參考歐盟《通用數據保障條例》第 4(12)條的定義。

者為減低危害風險而採取的補救行動，以及資料當事人應採取哪些行動以保障自己免受危害等。公署亦有計劃就通報機制提供範本和指引協助資料使用者作出通報。

(II) 資料保留時限

6. 目前，《私隱條例》的第二項資料保障原則訂明，資料使用者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。該原則未有界定個人資料何時為「不再需要」。我們留意到此做法與其他司法管轄區的資料保障法例相似，即沒有明確指明資料保留時限。

7. 保存資料時間越長，外洩的風險以及造成的影響會相應增加，保存應予刪除的個人資料會帶來不必要的私隱風險。然而，考慮到不同機構的服務性質和獨特需要，實際上難以在《私隱條例》中就不同機構為不同目的而持有的各類個人資料定下劃一的保留時限。因此，硬性設立劃一的資料保留期限未必合適。

8. 目前考慮的方向是透過修訂《私隱條例》，要求資料使用者制定一套清晰的個人資料保留政策，就其所收集的個人資料定下保留時限。保留資料政策應涵蓋多個方面，例如：不同種類的個人資料的最長保留時限；影響保留時限的相關法律規定，例如與稅務、

僱傭、某些特定專業(如法律和醫療)等相關的規例；保留時限的計算方法，例如在收集資料時、有關資料使用者停業時或與資料當事人結束會員關係時起計算等。

9. 現時《私隱條例》第五項資料保障原則(a)段訂明，資料使用者須採取所有切實可行的步驟，以確保任何人能確定資料使用者在個人資料方面的政策及實務。我們正考慮修訂第五項資料保障原則，明確要求資料使用者的個人資料政策須包含保留資料政策。資料使用者須確保會清晰告知有關人士該保留政策的詳細內容和會被有效執行。公署亦計劃提供資料保留政策範本和指引，供業界於制定和清晰列明資料保留政策時作參考。

(III) 懲處權力

10. 視乎不同的罪行，現時《私隱條例》中的刑事罰款包括第三級(港幣 1 萬元)、第五級(港幣 5 萬元)和第六級(港幣 10 萬元)罰款，全部均與《刑事訴訟程序條例》附表 8 罪行的罰款級數掛鈎[2]。

11. 目前，如公署發現資料使用者不遵循《私隱條例》所訂的資料保障原則，公署可向資料使用者發出執行

[2] 《私隱條例》第 35 條亦包括港幣 50 萬元和 100 萬元的刑事罰款，專門針對直接促銷的相關罪行。這些罰款專門針對包括無資料當事人同意下提供個人資料以供直接促銷、資料使用者首次將個人資料用於直接促銷時無通知資料當事人、將資料當事人的個人資料提供予直接促銷中使用等罪行。另外，《私隱條例》第 64 條亦包括港幣 100 萬元的刑事罰款，專門針對披露未經資料使用者同意而取得的個人資料的行為。

通知，要求糾正。如資料使用者在接獲執行通知後仍不遵循，可被處以罰款或監禁。不遵循執行通知一經首次定罪，最高可被判處第五級刑事罰款(即港幣5萬元[3])及最長可被判監禁2年。為反映罪行的嚴重性及提高《私隱條例》的阻嚇性，我們其中一個研究方向是提高相關刑事罰款。

12. 此外，我們留意到不少海外資料保障機構(如歐盟、新加坡、英國)均有權就違反其資料保障法例直接處以行政罰款。因此，我們亦正研究於香港引入直接行政罰款作為行政懲處措施的可行性。

13. 目前考慮的細節包括：

(a) 判處行政罰款的門檻：公署如獲授權判處行政罰款，須於判處罰款前考慮多方面的因素，從而決定是否判處罰款。可考慮的因素包括外洩的資料、資料外洩的嚴重性、資料使用者外洩資料的意圖和處理事故的態度、資料使用者所採取的補救行動，以及資料使用者過往的記錄等；

(b) 行政罰款的級數：我們參考了不同海外司法管轄區的做法，當中歐盟《通用數據保障條例》下的行政罰款最高可達2,000萬歐元(即約港幣1.78億元)，或公司對上一年全年全球營業額的4%，以較高者為準。我們正

[3] 不遵守根據《私隱條例》發出的執行通知而被定罪的案件中，法庭至今判處的罰款金額由港幣1,000元至5,000元不等。

研究引入與資料使用者全年營業額掛鈎的行政罰款的可行性，以及是否可以將不同規模的資料使用者按其營業額劃分，對應不同程度的行政罰款；

(c) 判處行政罰款的機制：公署須向資料使用者發出行政罰款通知，表明違反法例規定的情況、調查結果及罰款的指示水平，並應說明罰款的理由，以確保公署判處行政罰款的透明度。為提高判處行政罰款制度的公平性，資料使用者收到行政罰款通知後，應有合適的時間申述意見，並應有權就該通知向行政上訴委員會提出上訴。

(IV) 規管資料處理者

14. 目前，《私隱條例》把保障個人資料的責任施加予資料使用者，由資料使用者以合約方式，確保資料處理者[4]或分判商採取措施確保個人資料安全，而外判資料工作，例如把個人資料處理工作分判予其他服務供應商的做法愈見普遍。然而，現時《私隱條例》下沒有對資料處理者作出直接規管，因此有機會令到資料處理者忽略在處理資料的過程中防止外洩個人資料的重要性。將資料處理者納入法例監管有助提高保障，亦可使資料使用者和資料處理者公平分擔責任。

[4] 根據《私隱條例》第二項資料保障原則，「資料處理者」指代另一人處理個人資料及不為該人本身目的而處理該資料的人。

15. 我們參考了多個海外規管機構的做法，這些機構會直接規管資料處理者或要求資料處理者遵守某些特定(例如涉及保留和刪除資料，以及資料保安)的規定。目前研究的方向是直接規管資料處理者，向他們或分判商施加法律責任，例如要求資料處理者為個人資料的保留及其保安直接負責，並要求他們於發現資料外洩時向公署和資料使用者作出通報。

(V) 個人資料的定義

16. 根據《私隱條例》，現時「個人資料」的定義包括與「已識辨身分」人士有關的資料。考慮到現時追蹤和數據分析技術的廣泛應用，擴闊《私隱條例》中「個人資料」的定義以涵蓋與「可識辨身分」的自然人有關的資料，會更符合社會大眾對保障其個人資料的期望。我們參考了不同司法管轄區對「個人資料」的定義，當中不少均包括與「可識辨身分」的自然人有關的資料。我們認為修訂《私隱條例》中「個人資料」的定義能提高對個人資料的保障。

17. 有關上述幾個建議修例方向的海外規管制度摘要列載於**附件一**。

(VI) 規管披露屬於其他資料當事人的個人資料的行為

18. 除了上述由重大資料外洩事故引申出來的修訂條例事項外，我們對於過去一段時間社會上的「起底」

事件亦非常關注。公署自 2019 年 6 月 14 日至今共接獲及主動發現超過 4700 宗相關「起底」投訴及查詢個案，並已依法將超過 1400 宗相關「起底」個案交予警方作進一步調查。

19. 被「起底」人士遍及不同意見取向的人士和各行各業的從業員，包括警務人員及其家屬、政府官員及公職人員、曾表態支持或反對政府或警方的人士等。

20. 截至 2019 年 12 月 31 日，公署亦曾主動聯絡及超過 140 次去信相關的網站、網上社交平台或討論區的營運商要求移除超過 2500 條連結，其中接近七成已被移除。同時，公署亦要求涉事平台刊登警告字句，說明「起底」或網上欺凌行為有機會會觸犯《私隱條例》第 64 條。截至 2019 年 12 月 31 日，一共有 8 名人士因涉嫌違反該條文被警方拘捕。

21. 此外，律政司在 2019 年 10 月 25 日向法庭取得禁制令，禁制任何人在沒有相關人士的同意下及同時有意圖或相當可能會恐嚇、騷擾、威脅或煩擾相關人士的情況下使用、發布、傳達或披露屬於警務人員或其家屬的個人資料；恐嚇、騷擾、威脅或煩擾警務人員或其家屬；或協助、煽動、教唆或授權他人從事上述等行為。截至 2019 年 12 月 31 日，公署共將 40 宗接獲及發現涉嫌違反法庭禁制令的個案轉介予律政司跟進。

22. 政府現正研究如何修訂《私隱條例》以便更有效遏止「起底」行為，其中的考慮方向包括:考慮修訂條

文以更針對性地處理與「起底」有關的行為、賦予專員法定權力要求社交平台或網站移除涉及「起底」的內容，以及賦予專員刑事調查及提出檢控的權力等。

徵求意見和未來路向

23. 請委員備悉本文件的內容，並就上述建議的方向提供意見。

24. 在聽取委員會的意見後，我們會與公署進一步深入研究具體修例建議，並會適時諮詢相關持份者包括本事務委員會。

政制及內地事務局
二零二零年一月

附件一

其他司法管轄區的相關規管制度摘要

資料外洩通報機制

a. 向監管機構/受影響人士通報的門檻

澳洲	向監管機構通報的門檻：當資料被未經許可地讀取或披露，而一個合理人士認為該未經許可的讀取或披露很可能導致與該資料有關的個人蒙受嚴重損害時，便須通報。 向受影響人士通報的門檻：當資料被未經許可地讀取或披露，而一個合理人士認為該未經許可的讀取或披露很可能導致與該資料有關的個人蒙受嚴重損害時，便須通報。
加拿大	向監管機構通報的門檻：機構合理地相信發生的資料外洩事故對個人造成「重大損害的真正風險」。 向受影響人士通報的門檻：機構合理地相信發生的資料外洩事故對個人造成「重大損害的真正風險」。
歐盟	向監管機構通報的門檻：除非某資料外洩不太可能對自然人的權利和自由構成風險，否則機構須向有關監管機構通報資料外洩。 向受影響人士通報的門檻：當個人資料外泄事故很可能對自然人的權利及自由造成高度風險。
新西蘭	向監管機構/受影響人士通報的門檻：可合理地相信資料外洩事故已或有可能會對受影響人士造成嚴重損害。

	(有待議會討論的私隱草案[5])

b. 通報的時限

澳洲	向監管機構通報的時限:在切實可行的範圍內盡快通報。根據監管機構發出的指引，資料使用者可於知悉有懷疑資料外洩起計的 30 日內，為通報事故作評估。 向受影響人士通報的時限:在切實可行的範圍內盡快通報。
加拿大	向監管機構通報的時限:在可行的範圍內盡快通報。 向受影響人士通報的時限:在可行的範圍內盡快通報。
歐盟	向監管機構通報的時限:不可有不當延誤，而如情況可行時，在知悉資料外洩後不多於 72 小時內通報。《通用數據保障條例》容許資料使用者於沒有不當進一步延誤的情況下，分階段提供所需資料。 向受影響人士通報的時限:不可有不當延誤。
新西蘭	向監管機構通報的時限:在切實可行的範圍內盡快通報。 (有待議會討論的私隱草案) 向受影響人士通報的時限:在切實可行的範圍內盡快通報。 (有待議會討論的私隱草案)

[5] 有關《2018 年私隱草案》於 2019 年 8 月 7 日在議會進行二讀。草案將會進入全體委員會進行討論和審議。

c. 通報的方式

澳洲	向監管機構通報的方式:資料使用者須向監管機構作出網上通報。 向受影響人士通報的方式: 資料使用者須直接向受影響人士通報。如直接向受影響人士通報不是切實可行，資料使用者須於其網頁發報一份聲明(即向監管機構作出的通報)的副本，並採取合理的步驟，把該聲明的內容通知有嚴重損害風險的人士。
加拿大	向監管機構通報的方式:資料使用者須以書面或可以任何安全穩妥的通訊方式作出通報。 向受影響人士通報的方式:資料使用者須親身、以電話、郵遞、電郵、或其他通訊形式作出直接通報。如直接通知很可能會對受影響人士造成進一步損害、對機構帶來困難或機構沒有受影響人士的聯絡資料，機構可作出間接通報。間接通報須以公開通訊或類似措施作出。
歐盟	向監管機構通報的方式:個別成員國的資料保護法例可進一步規定通報的形式。 向受影響人士通報的方式:資料使用者須向受影響人士作出直接通報。如直接通報涉及不成比例的工作，替代的通報形式須以公開通訊或類似措施，而藉有關措施可同樣有效的方式向受影響人士作出直接通報。可接受的通報方式包括電郵、短訊、郵遞、顯眼的網頁橫額或通知、印刷媒體的顯眼廣告等。

新西蘭	向監管機構通報的方式:監管機構會在私隱草案通過後就通報方式及要求提供指引。 向受影響人士通報的方式:如無法在合理地切實可行的情況下向受影響人士或受影響個別人士所屬群組的成員通報，資料使用者須發出公眾通知。 (有待議會討論的私隱草案)

d. 未能作出通報的後果

澳洲	法人團體干涉個人私隱可被判處高達 210 萬澳元的民事罰款。
加拿大	機構可被法庭判罰刑事罰款最高 10 萬加元。
歐盟	高達 1,000 萬歐元或機構全球年度營業額的 2%，以較高者為準。除行政罰款外，監管機構可施加於《通用數據保障條例》第 58 條提述的其他懲罰措施。
新西蘭	在沒有合理辯解的情況下未能向私隱專員通報，可被法庭判罰刑事罰款最高 1 萬新西蘭元。 (有待議會討論的私隱草案)

資料保留時限

a. 規管資料保留時限的條文

澳洲	機構應視乎情況採取合理的措施，銷毀「不再需要」用於獲許可目的的個人資料。
加拿大	保留個人資料的時限只應為滿足原來的收集目的所必要的時間。機構(資料使用者)應制定指引，列明資料保留的最長和最短時間。
歐盟	不得保留個人資料至超過原來處理目的所需的時間。
新西蘭	機構(資料使用者)不得保留個人資料至超過原來合法地使用資料的目的所需的時間。
新加坡	當機構(資料使用者)可合理地認為不再需要為法律、商業或其他收集目的而保留個人資料時，便應停止保留該資料。

懲處權力

a. 監管機構處以行政罰款的權力

澳洲	沒有
加拿大	沒有
歐盟	有。違反《通用數據保障條例》可被處以兩級行政罰款，須視乎違規事故的性質。條例亦訂明監管機構須根據一系列考慮因素決定是否處以行政罰款和罰款金額的水平。會員國的監管機構具酌情權選用最合適的懲處措施，決定有關個案是否處以行政罰款。
英國	有。英國資訊專員辦公室有權處以罰款(在《通用數據保障條例》實施前已適用)。
新西蘭	沒有
新加坡	有。只會在糾正指令不足以反映違規事故的嚴

	重性時，才會處以罰款。

b. 懲罰水平

澳洲	澳洲資訊專員無權處以行政罰款，但可就嚴重和重犯的私隱相關案件向法庭申請民事罰款。個人可被處以高達 42 萬澳元的罰款，商業機構則可被處以高達 210 萬澳元的罰款。
加拿大	不適用
歐盟	未能遵守《通用數據保障條例》的資料使用者／資料處理者可被處以： (i) 高級：高達 2,000 萬歐元或機構對上一年全球全年營業額 4%的行政罰款，以較高者為準； (ii) 次級：高達 1,000 萬歐元或機構對上一年全球全年營業額 2%的行政罰款，以較高者為準。
新西蘭	不適用
新加坡	如機構未能遵守資料收集、使用、披露、存取、更正和保護的規定，資料保障監管機構有權指令機構繳付最高 100 萬坡元的罰款。

規管資料處理者

a. 有否直接規管資料處理者

澳洲	有
加拿大	有
歐盟	有
新西蘭	有
新加坡	有 (只適用於個人資料保安安排規定和保留規定)

b. 規管資料處理者的方式

澳洲	參與處理個人資料的機構，在收集、保留、使用或披露個人資料等方面均受《1988 年私隱法案》規管。
加拿大	資料處理者受直接和間接規管。 ● 直接規管：資料保障法例(《個人資料保護及電子文件法令》)適用於所有於商業活動中收集、使用或披露個人資料的機構。 ● 間接規管：將個人資料轉移予資料處理者處理的資料使用者，須以合約或其他方式，確保資料處理者在處理資料時，資料獲得相若程度的保障。
歐盟	資料處理者受直接和間接規管。 ● 直接規管：資料處理者須保存處理活動記錄、根據資料控制者的指示處理資料、保障個人資料的保安、盡快向資料控制者通報資料外洩事故和委任資料保障主任、遵守跨境資料轉移的相關條文等。 ● 間接規管：《通用數據保障條例》要求資料控制者委任或選用能在技術及機構層面的措施上提供足夠保障和符合條例規定的資料處理者。資料控制者須以合約規範方法，將指定條文納入與資料處理者簽訂的合約中。
新西蘭	持有或處理個人資料的個人或機構須遵守《1993 年私隱法令》。
新加坡	資料處理者受直接和間接規管。 ● 直接規管：保護個人資料的責任直接適用於資料處理者，其中包括為個人資料提供合理的保安安排規定和保留規定。 ● 間接規管：資料處理者亦受其與資料使用者之間的合約間接規管。資料使用者仍須

	對資料處理者處理個人資料的行為負上法律責任，亦應確保資料處理者的資料處理工作符合《2012 年個人資料保護法令》的規定。

個人資料的定義

澳洲	不論真確與否及有否以實質形式記錄，有關一名已被識辨的人士或可合理地被識辨的人士的資料或意見。
加拿大	有關一名可被識辨的人士的資料。
歐盟	有關一名已被識辨或可被識辨的自然人的任何資訊。 「可被識辨的自然人」指可直接或間接地被識辨的自然人，尤其透過參考： (a) 標識符例如姓名、位置資料或網上標識符；或 (b) 該名個人的身體、生理、基因、精神、經濟、文化或社交身分所特有的一個或多個因素。
新西蘭	有關一名可被識辨的人士的資料。
新加坡	不論資料真確與否，可以從(a)該資料，或(b)該資料及機構有權或可能取閱的其他資訊中識辨某人的資料。