

**2019年5月22日立法會會議上
通過的「追上科技發展，加強保障市民私隱」議案**

進度報告

目的

在2019年5月22日的立法會會議上，由梁美芬議員動議，經葛珮帆議員修正的「追上科技發展，加強保障市民私隱」議案獲得通過。已獲通過的議案全文見附件。本文件旨在匯報相關工作的進展。

檢討《個人資料(私隱)條例》的工作

2. 資訊科技迅速發展，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趨勢由過往有關不當收集和使用個人資料、直接行銷等，至近年較多變成與資料保安相關，包括個人資料外洩、保安系統出現漏洞以致受到黑客入侵等問題。加上較早前發生的一系列重大個人資料外洩事故，令公眾越來越關注《個人資料(私隱)條例》(《私隱條例》)是否足以保障個人資料私隱。

3. 政府高度重視個人資料私隱的保障，亦同意在保障私隱方面需要與時並進。我們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》。公署日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。

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，但現行法例並無強制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。引入強制通報機制能確保私隱專員得以監察該等機構處理事故的做法，而該等機構亦可向私隱專員尋求指示作跟進，以減低或防止其因事故而蒙受進一步損失。我們認為引入強制通報機制有助加強對個人資料的保障。

5. 就研究設立強制性個人資料外洩通報機制方面，我們目前考慮的課題包括“個人資料外洩”的定義和通報的門檻(即機構遇到甚麼類型和規模的資料外洩事故才需要通報公署和資料當事人，而向兩者作出通報的門檻又應否一樣)等。我們參考了海外經驗，就通報門檻而言，機構考慮是否應向公署通報資料外洩事故時，可以參考不同的因素，包括外洩個人資料的類別、涉及個人資料的數量、發生身分盜竊的可能性、外洩資料是否有足夠加密等。

6. 就通報時限而言，海外經驗顯示，資料使用者或需時間核實資料外洩個案的詳細情況。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。

資料保留時限

7. 《私隱條例》的第二項資料保障原則訂明，資料使用者須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。此做法與其他司法管轄區的資料保障法例相似。

8. 然而，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，保存早該刪除的個人資料亦會帶來不必要的私隱風險。考慮到不同機構的服務性質和獨特需要，硬性設立劃一的資料保留期限可能未必合適。因此，我們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。

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”。我們會研究應否修訂第五項資料保障原則以要求資料使用者明確列出其保留資料政策。

懲處權力

10. 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通知，要求糾正。違反資料保障原則本身並不構成罪行，只有在接獲執行通知後仍不遵循才屬犯罪，

可被處以罰款或監禁。不遵循執行通知一經首次定罪，可被判第五級刑事罰款(按照《刑事訴訟程序條例》附表 8 的罰款級數，即最高 5 萬港元罰款)及最長可判監禁 2 年。根據經驗，《私隱條例》現時所訂的刑事罰款，阻嚇性不足以令資料使用者遵守《私隱條例》的規定。為提高《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。

11. 此外，我們留意到不少海外資料保障機構均有權就違反其資料保障法例處以行政罰款。因此，我們亦正研究於香港引入直接行政罰款的可行性。

規管資料處理者

12. 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¹或分判商採取措施確保個人資料安全。換言之，《私隱條例》對資料處理者只實施間接規管。然而，隨着科技發展，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。我們原則上認為有需要監管資料處理者，以加強保障處理中的個人資料，亦可使資料使用者和資料處理者公平分擔責任。

13. 我們留意到多個海外規管機構會直接規管資料處理者或要求資料處理者遵守有關某些情況(如保留和刪除資料，以及資料保安)的規定。因此，我們的研

¹ 根據《個人資料(私隱)條例》，“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。

究方向是向資料處理者作出直接規管，向資料處理者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。

個人資料的定義

14. 根據《私隱條例》，“個人資料”現時的定義包括與“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，更能滿足社會的需要和期望。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”²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。

未來路向

15. 我們會與公署進一步深入研究上述修例建議方向的可行性，並參考其他司法管轄區的相關私隱條例和香港的實際情況，適時諮詢相關持份者包括立法會相關事務委員會的意見，以期盡快就修訂《私隱條例》提出具體的建議。

政制及內地事務局

二零一九年九月

² “可識辨身分的人”是指一名可透過身分標識符(如姓名、位置或網上標識符)，直接或間接被識辨身分的在世的個人。

2019 年 5 月 22 日的立法會會議
梁美芬議員就“追上科技發展，加強保障市民私隱”
動議的議案

經葛珮帆議員修正的議案

本港現時保障個人私隱的法例不全面，特別是沒有針對性規管以網絡儲存個人私隱資料的法例，而保護兒童網絡私隱方面亦欠缺專門法例，以致未能阻嚇不法分子利用網絡收集兒童私隱資料及侵犯兒童私隱，甚至藉此作出猥褻行為；本港多次發生大規模個人私隱資料外泄的嚴重事故，例如 2009 年八達通卡有限公司被揭發將 240 萬客戶資料轉售給其他公司作推廣用途、2017 年選舉事務處遺失載有全港 378 萬名地方選區選民個人資料的手提電腦、2018 年國泰航空公司泄漏 940 萬乘客個人資料；《個人資料(私隱)條例》在 1996 年生效，政府僅在 2012 年對該條例作出一次修訂，隨着互聯網、社交媒體、大數據、人工智能等科技發展一日千里所帶來的私隱風險及歐盟《通用數據保障條例》生效，更加顯得《個人資料(私隱)條例》落後及對個人資料私隱保護明顯不足；就此，本會促請政府追上科技發展，全面檢討保障個人資料私隱的政策，以加強保障市民私隱；有關建議包括：

(一) 參考其他司法管轄區在保護網絡私隱方面的各項措施及法例，包括限制儲存網絡資料的保障及規定，以及通報事故機制等，以制定適用於本港的網絡私隱保護法；

(二) 參考其他司法管轄區的法例，制定保護兒童網絡私隱的專門法例，包括訂立限制網絡營運商過分收集及儲存兒童私隱資料，以及防止侵犯兒童私隱等規定，藉此有效保障兒童的個人私隱；

(三) 參考歐盟《通用數據保障條例》及其他司法管轄區的相關法例，從速全面修訂《個人資料(私隱)條例》，包括要求資料使用者須在指定期限內向個人資料私隱專員(‘私隱專員’)及資料當事人通報資料外泄事故及提高違反執行通知罰則以加強阻嚇力；

(四) 就個人私隱資料外泄的嚴重事故，研究設立更有效的賠償及授權私隱專員執行行政處罰(例如罰款)等機制，以保障市民權益和促使資料使用者提升對個人資料的保護；

(五) 針對部分企業要求客戶使用服務前需提交與服務無關的個人資料的問題，檢討現行資料使用者可收集個人資料的範圍，包括界定何謂敏感個人資料，並就收集及儲存敏感資料設定限制，以加強保護市民個人資料；

(六) 要求所有政府部門和公私營機構檢討處理個人資料的政策和保安措施，以免再發生市民個人資料私隱遭侵害的事故；及

(七) 加強公眾宣傳，以提高市民及公私營機構對保護和尊重個人資料私隱的認識和關注。