

對抗新型冠狀病毒疫情 給僱主和僱員的私隱指引

新型冠狀病毒疫情持續，令僱主關注是否可以收集僱員的健康數據，以幫助監察和預防在工作場所及社區傳播病毒。疫情期間，許多公共及私人機構都推行了在家工作安排，以減低社交接觸。很多僱主和僱員因此在家進行在線商務會議，而個人資料私隱外洩的可能性也需要高度關注。

在家工作同時意味著更多錯誤可能會發生，包括一些低技術錯誤例如便攜式裝置被盜竊或遺失、資訊科技人員面對更大壓力，以及網絡犯罪者乘機以虛假的健康警報以傳送竊取密碼的惡意郵件或軟件。香港個人資料私隱專員公署的私隱專員呼籲僱主和僱員，在這段時間保持警惕。

公共衛生事件 與個人資料的關係

重大公共衛生利益

世界衛生組織於2020年1月30日宣布新型冠狀病毒爆發為國際關注的突發公共衛生事件，並於2020年3月11日定性為「全球大流行疫情」。現時本地及全球均有急切需要控制病毒的傳播，重大公共衛生及安全利益，應屬所有人包括資料使用者的首要關注。

保障資料的原則不應阻礙對抗新型冠狀病毒的措施，但機構亦不應輕視其在處理個人資料時的責任。

《私隱條例》中與突發公共衛生事件有關的豁免

根據《私隱條例》第59(1)條，當個人資料的使用與保障資料當事人或任何其他人的健康有關，而若遵從《私隱條例》附表一的保障資料第3原則（資料的使用）的管限會對資料當事

人或任何其他人的健康造成嚴重損害，該個人資料的使用可能獲豁免而不受此管限。換句話說，如能展示使用資料是出於保障個人及整體公共衛生，即使因未經同意而使用相關資料而出現違規的情況，亦可能得以免責。而《私隱條例》第59(2)條更指出，在相當可能會對資料當事人或任何其他人的身體或精神健康造成嚴重損害的情況下，資料使用者可毋須得到資料當事人的同意而向第三者披露關乎某資料當事人的身分或位置的個人資料。

平衡私隱與公共衛生需要

個人資料私隱權並非絕對的權利。事實上，它可能會受到其他與其有衝突的權利或利益所約束，例如屬絕對權利的個人生存權和公眾利益（包括公共衛生）。

根據(i)《香港人權法案條例》第II部第二條，和(ii)《公民權利和政治權利國際公約》第6條，「生存權」是指人人皆有天賦之生存的權利。聯合國人權事務委員會在2018年11月亦指出，「生存權是享有所有其他人權的前提」，

並將「生存權」定義為「最高等權利」。此權利屬絕對性，並凌駕於其他可能與其有衝突的基本人權，包括私隱權。生存權不僅指資料當事人的生存權，例如新型冠狀病毒的潛在帶病毒者，亦包括社會上的其他人。

突發公共衛生事件下 僱主和僱員的常見私隱問題

僱主可以收集僱員的體溫測量 或其他健康數據嗎？

僱主有法律及企業責任去保障僱員及訪客的健康。在新型冠狀病毒下，為了保障僱員及訪客的健康，僱主收集他們的體溫測量數據或屬新型冠狀病毒醫學症狀的有限資訊，一般而言屬合理的做法。

僱主可收集哪類個人資料， 以及如何正確地收集？

僱主在收集資料時必須遵守的一般規定是，收集的資料應該是**必要、適當及與達到的目的相稱**。他們應先以匿名或刪除可識別資料的方式處理相關資料，以侵犯最少私隱的措施為首選。

一般而言，自我申報機制較無差別地收集健康數據的全面強制機制更為可取。僱主應向僱員說明如何處理收集到的資料。如現有的私隱聲明中未涵蓋該類資料的收集，則必須在收集資料時或之前向僱員提供一個新的《收集個人資料聲明》，以告知僱員所收集的資料及其目的（例如保障公共衛生）及資料可能會轉移給哪類人士（例如公共衛生機關）。作為良好的道德規範，在《收集個人資料聲明》中應告知僱員有關資料將被僱主保留多久。

外遊紀錄如何？

僱主可要求僱員提供外遊資料嗎？

《個人資料（私隱）條例》（下稱：《私隱條例》）沒有禁止任何機構收集他人的外遊資料。鑑於本地及全球的新型冠狀病毒確診個案仍不斷出

現，以及僱主提供安全工作環境的法律及企業責任，僱主向從海外（特別是高風險地區）回港的僱員收集外遊資料實屬合理。一如健康數據，外遊資料的收集應針對特定的目的，並應收集最少的資料，而自我申報機制亦比全面強制申報機制更可取。

可以把收集的個人資料向其他人披露、 或用作其他目的嗎？

除非得到相關人士自願給予的明示同意，或《私隱條例》下的豁免適用，否則僱主不得將為對抗新型冠狀病毒而收集的個人資料披露或使用作其他無關的目的。

為了保障公共衛生，如僱主僅為了追蹤和治療感染者，及因有迫切需要追蹤其緊密接觸者，向政府或衛生機構披露他人的身份、健康狀況及位置資訊，並不會被視為違反《私隱條例》（即保障資料第3原則）。

如僱員不幸感染新型冠狀病毒，僱主可在**不透露**感染者的個人身份信息下通知其他員工、訪客及物業管理處，例如發出告示說明有員工受感染已足夠。在大多數情況下，於告示中披露受感染僱員的名字及其個人資料會被視為不必要或不相稱。

收集的個人資料可以被保留多長時間？

在已達致收集目的後，如經過一段合理時間亦沒有證據說明僱員感染新型冠狀病毒，或與感染者有密切接觸，僱主應永久銷毀為對抗新型冠狀病毒而收集的個人資料。

在僱員的醫療及健康數據方面， 僱主應注意甚麼資料保安問題？

僱主應採取所有可行的步驟（例如把資料存放於上鎖的櫃中、對資料進行加密並僅允許獲授權人士存取資料），以保障所收集的個人資料免遭未經授權或意外的存取、處理、刪除、遺失或使用。由於醫療或健康數據被視為較敏感資料，而外洩資料可能對相關人士造成重大傷害，因此足夠的資料保安措施尤其重要。

於大流行疫情期間，僱主應為僱員在家工作採取甚麼樣的安全措施？

個人資料的保障不應妨礙在家工作安排，但僱主及僱員在遠離有專業管理的工作環境下，處理轉移或使用文件和數據時要格外小心，以免發生如網絡攻擊或遺失便攜式裝置等事故。網絡犯罪者可能會藉員工分散，把竊取密碼的惡意郵件或軟件偽裝成健康警報，滲透到機構中。以下是在家工作的一些切實可行的措施以保障個人資料的安全。

由辦公室轉移文件或電腦檔案至家中前：

1. 先向上司尋求指示或批准；
2. 盡量減少由僱主的處所及資訊系統轉移至外間的資料；
3. 採取所有可行的步驟，以保障個人資料免遭未經授權或意外的存取、處理、刪除、遺失或使用，尤其是須注意：
 - 資料的種類及可能造成的損害
 - 資料存放的實體地點
 - 存放資料的設備是否已採取任何保安措施
 - 任何確保能查閱資料的人員具備良好操守、審慎態度及辦事能力的措施
 - 任何可確保安全傳送資料的措施；
4. 由僱主的處所轉移至外間前，將個人資料／保密資料纂輯；
5. 在使用便攜式裝置儲存及轉移資料前，必須得到上司批准及將儲存的文件加密；

6. 將數據加密；
7. 在特別情況下，在運送期間將文件或裝置與運送者緊緊；及
8. 記錄資料的轉移歷程並保存記錄。

此外，在家工作並使用自己裝置的僱員，要小心留意有關網絡保安以防資料外洩。以下是一些有關的保安建議：

9. 使用多重身份認證；
10. 不要和其他人共用工作裝置的帳戶；
11. 確保無線安全；
12. 定期更改密碼；
13. 安裝適合的防病毒軟件；
14. 為裝置定期進行系統更新；
15. 選擇私隱友好的設定，例如進行在線會議時，不允許錄製視頻或音頻。禁用任何關注追蹤功能；及
16. 在開始會議之前務必驗證在線會議的參與者身份。

最後，當僱員發現可疑的網站或接獲可疑的電子郵件時，他們：

17. 切勿點擊網頁鏈結及下載文件或應用程式。相反，他們應向有關組織或當局核實其真確性；及
18. 在發送或上載文件之前，應一再仔細檢查要發送的內容和收件人的身份。■

如欲了解更多有關個人資料私隱的資料，可聯絡香港個人資料私隱專員公署。

電話：+852 2827 2827

電郵：enquiry@pcpd.org.hk

傳真：+852 2877 7026

網址：www.pcpd.org.hk

