Chinese Traditional

information and privacy commission new south wales

資訊介紹

2023年11月

MNDB計劃常見問題解答

本文爲誰提供資訊？	本文供新南威爾士州的公眾瞭解有關資料外洩強制通報計劃 (Mandatory Notification of Data Breach Scheme，簡稱：MNDB計劃) 的詳情。
爲甚麼這些資訊很重要？	本資料幫助你詳細瞭解資料外洩強制通報計劃，以及你在受到資料外洩事件影響後可行使的權利。

甚麼是資料外洩強制通報計劃？

新州公共機構在發生資料外洩事件並且該外洩屬“須通報事件”時，必須依據《1998年私隱和個人資訊保護法》(*Privacy and Personal Information Protection Act 1998*，簡稱：PPIP法) 規定通報。

MNDB計劃何時生效？

MNDB計劃於2023年11月28日正式生效施行。

MNDB計劃適用於哪些機構？

MNDB計劃適用於新州公共部門的機構、部長辦公室、大學、地方議會政府，以及不受聯邦私隱法管轄的州政府所有企業。

甚麼是資料外洩應對政策？

資料外洩應對政策 (Data Breach Policy，簡稱：DBP) 由一系列書面政策或計劃組成，規定了公共機構在發生資料外洩事件後應該採取的應對措施。法律規定所有公共機構必須制定各自的DBP。DBP必須確定公共機構內部人員在管理資料外洩方面的角色與職責，以及在資料外洩事件發生時應該遵循的處理步驟。

公共機構必須確保公眾能夠自由獲取其DBP。換言之，公共機構需要在網站上發佈DBP。

甚麼是須通報資料外洩事件？

MNDB計劃規定，任何公共機構在發生屬於須通報資料外洩事件後，必須向私隱專員 (Privacy Commissioner) 報告。

有以下情況的資料外洩即屬於“須通報事件”：

- 未經授權訪問或披露公共機構持有的個人資料，並可能對此等資料涉及的個人造成**嚴重傷害**。
- 疑似在未經授權訪問或披露的情況下導致公共機構持有的個人資料承受損失，並可能對此等資料涉及的個人造成**嚴重傷害**。

甚麼是嚴重傷害?

嚴重傷害可以包括身體、經濟或物質傷害，情感或心理傷害，或名譽傷害。傷害導致的影響因人而異，但是可能包括：

- 因詐騙造成經濟損失；
- 可能帶來有害身心健康的風險，例如受到來自曾經施虐的前伴侶的傷害；
- 因個人身份資料遭到盜竊而影響你的財務以及/或者信用記錄；
- 嚴重損害個人名譽。

爲何會發生資料外洩？

籠統而言，人為錯誤、系統故障，或惡意及違法網路入侵等，都可能導致資料外洩。

哪些情況可能導致資料外洩？

部份導致資料外洩發生的情況包括：

人爲錯誤：

- 信件或電子郵件發送給錯誤的收件人；
- 錯誤地向未經授權或密碼保護不足的人員授予系統訪問權；
- 文件檔案、手提電腦、USB或電話等存儲有個人資料的實物資產丟失或放錯地方。

系統故障：

- 編程錯誤，導致無需身份驗證即可訪問系統或自動生成通知；
- 沒有彌補系統的已知漏洞或使用支持補丁予以維護。

惡意或違法入侵：

- 勒索軟體、惡意軟體、駭客攻擊、網路釣魚、暴力破解攻擊等網路事件；
- 利用社會工程或冒充手法，導致個人資料不恰當地受到披露；
- 來自機構內部的威脅，包括僱員使用有效登錄憑證，在其職權或授權範圍之外調用或披露其他人的資料。

公共機構是否必須通知私隱專員？

如果經評估資料外洩屬須通報事件，相關機構必須立即使用IPC網站提供的專用表格，通知私隱專員。

須通報資料外洩事件發生後，我是否會收到通知？

如果公共機構確定其發生的資料外洩屬須通報事件，並涉及你的個人資料，則必須盡快通知你。這意味著，公共機構必須以書面形式向你告知資料外洩事件，同時提供相關資訊，包括：

- 該機構已經採取或計劃採取的行動，從而控制或減少對你造成傷害；
- 你在資料外洩事件發生後應該考慮採取的應對措施；
- 如何要求對公共機構的行為進行內部審查或如何向私隱專員提出投訴的資訊。

我將在資料外洩事件發生多長時間後才會收到通知？

當公共機構有合理的理由懷疑資料可能遭到外洩，並且該外洩屬於須通報事件，他們必須採取以下措施：

- 盡一切合理努力，遏制違法行為；
- 評估該機構在過去30天內是否存在未經授權的系統訪問、資訊披露或個人資料遭受損失的情況；
- 評估過去30天內是否有可能對任何受影響的個人造成了嚴重傷害；
- 盡一切合理努力，減少疑似違法行為造成的損害。

如果完成上述步驟後，公共機構確定其發生的資料外洩屬於須通報事件，同時你的個人資料受到影響，則必須盡快通知你。

公共機構沒有我的聯絡詳情而無法通知資料外洩事件，我應該怎麼辦？

MNDB計劃賦予各公共機構共享資訊的權力，從而使他們能夠向另一個公共機構索取相關的個人資料。公共機構僅可要求獲取用於確認受資料外洩事件影響的個人的姓名及其聯絡方式等合理必要的資訊。

但是，如果發生資料外洩的機構無法直接通知你，他們必須在其網站上發佈通知，同時採取合理措施廣而告之。通知必須在機構的公共通知登記檔案頁上保留至少12個月。

公共機構是否可有任何理由不通知我？

是的。在部份例外情況下，公共機構可以不通知受資料外洩事件影響的個人。例如，涉事機構迅速採取補救措施，並由於這些措施致使資料外洩可能沒有造成嚴重傷害。在這種情況下，他們無需通知任何受影響的個人。

涉事機構通知我之後是否還會提供其他幫助？

取決於資料外洩事件的具體情況，涉事機構在通知你之後，還有可能提供其他類型的協助與支援。例如：

- 協助更換駕駛執照等受資料外洩事件影響的政府官方身份證件或文件；
- 提供保護個人資訊的建議；
- 提供其他支援以及輔導服務。

我收到通知後應該做些甚麼？

你可以採取一些具體實用的措施，保護你的個人資料，並降低資料外洩事件可能為你帶來的傷害風險。這些措施將取決於資料外洩發生的情況以及事件所涉及的資料類型。你收到的通知應該建議可以針對已獲識別的外洩資料類型採取哪些行動。

如果你需要獲得有關資料外洩事件的詳情，或希望瞭解如何更好地保護自己的個人資訊，可以聯絡向你發出通知的機構。

如何獲得更多資訊？

你可以在資訊和私隱委員會 (IPC) 的官方網站上找到更多資訊以及其他資源。你也可以透過以下方式聯絡IPC。

獲取更多資訊

聯絡新州資訊和私隱委員會(Information and Privacy Commission NSW - IPC)：

免費電話： 1800 472 679

電郵： ipcinfo@ipc.nsw.gov.au

網址： www.ipc.nsw.gov.au

注意：本文資訊僅供參考。個人應該就具體情況獲取法律建議。