Chinese (Traditional) | 繁體中文

2023 年私隱影響評估摘要
（Summary of the 2023 Privacy Impact Assessment）

國家殘障數據資產系統和澳洲全國數據整合基礎設施

社會部（Department of Social Services）目前與澳洲統計局（Australian Bureau of Statistics）和澳洲醫療福利協會（Australian Institute of Health and Welfare）共同建立國家殘障數據資產系統。以上三大澳洲政府機構稱之為聯邦合作夥伴（Commonwealth Partners）。

各州份和領地與殘障社群亦介入制定殘障數據資產系統。國家殘障數據資產系統委員會（National Disability Data Asset Council）（簡稱「委員會」）負責監督殘障數據資產系統的使用，並涉及到與政府界別及殘障社群分享決策過程。殘障數據資產系統從不同政府機構收集無法識別個人身份、與全體澳洲人相關的資訊，從而深入了解為殘障人士營造的成效。

支援殘障數據資產的基本系統屬於澳洲國家數據整合基礎設施（Australian National Data Integration Infrastructure）。此系統讓我們連接及分析殘障數據資產系統內的數據。澳洲國家數據整合基礎設施董事會（簡稱「董事會」）負責監督公眾如何使用此系統。

詳情載於國家殘障數據資產系統（National Disability Data Asset）網站上，當中包括國家殘障數據資產系統私隱（Privacy for the National Disability Data Asset）方面的資訊。

何謂私隱影響評估？

私隱影響評估（Privacy Impact Assessment，下文簡稱「PIA」）旨在檢閱項目及如何潛在影響公眾私隱。PIA 就管理、減少或移除私隱方面的風險和影響提出不同建議。Maddocks 私隱專業人員為國家殘障數據資產及其基本系統執行了 PIA。

Maddocks 編撰了詳盡的 PIA 報告。此份文件屬於另一份報告之摘要，當中包括了不同結果及建議的流程和概覽。

詳情載於國家殘障數據資產系統網站上的國家殘障數據資產系統私隱（Privacy for the National Disability Data Asset）頁面。

聯邦合作夥伴計劃於 2025 年更新 PIA。

評估流程

2023 年編撰之 PIA：

- 檢查殘障數據資產及其基本系統是否與澳洲的《1988 私隱法》（Privacy Act 1988）達成一致，當中包括澳洲私隱準則，即涉及如何管理個人資料的法律。
- 留意到任何私隱風險以及我們可減少風險的方式
- 協助我們管理項目出現的任何私隱風險和影響
- 審核殘障數據資產系統如何保障個人資料，包括濫用、遺失，或者由未經授權的人士獲取、變更或分享資訊。

聯邦合作夥伴與 Maddocks 就 PIA 一事於 2023 年 3 月至 7 月諮詢各利益相關者的意見。150 多人出席了以上的諮詢環節。澳洲聾盲人士倡議服務機構（Deafblind Australia）與殘障人士協助舉辦了兩場諮詢環節。澳洲唐氏綜合症聯盟（Down Syndrome Australia）協助澳洲共融高峰機構（Inclusion Australia）與智力障礙人士舉辦了一場諮詢環節。

Maddocks 就意見回饋編撰了詳盡的諮報告。報告的摘要載於國家殘障數據資產系統私隱（Privacy for the National Disability Data Asset）頁面。

結果摘要

公眾於諮詢環節表達對殘障數據資產系統的制定工作強烈支持。某些人士指出未經授權而分享健康或殘障狀況的資訊對公眾造成的嚴重問題。

相比其他個人資料，澳洲社會期望敏感資訊應給予更多保障。敏感資訊可能包括與個人健康、種族或族裔及宗教信仰相關的資訊。詳情及其他例子載於《私隱法》（Privacy Act）第六節及澳洲資訊委員會辦事處（Office of the Australian Information Commissioner）網站。

於殘障數據資產系統設計部分，Maddocks 留意到聯邦合作夥伴聚焦於私隱方面。特別是管理方面的安排強而有力之外，更鉅細無遺。有不同規則施加於項目決策者及決策方式。以上規則及流程已獲精心設計，以管理數據和項目的私隱風險，當中包括發現日後出現的危害。

聯邦合作夥伴會落實不同流程，以保障公眾的個人資料。連結不同數據期間，當中包括：

- 使用詳盡的數據分享協議
- 遵循數據分享的法律，包括《2022 年數據可用度及透明度法》（Data Availability and Transparency Act 2022）
- 於連結數據可分享的內容中備有既定規則例如，發布研究結果前檢查內容

我們會於殘障數據資產系統內移除無法識別個人身份的資訊，讓外界無法得知當事人的身份。但利益持有者於諮詢環節留意到，連結數據期間，可能會易於讓他人重新識別當事人的個人身份。因應更多數據加入至殘障數據資產系統，如此重新識別個人身份資訊的風險可能會增加。

Maddocks 建議採取不同方法應對以上風險，並改善保障公眾私隱的做法。

建議

PIA 建議列於以下主題：

1. 日後將數據集增添至殘障數據資產系統的準則
2. 數據服務提供者收集通知書
3. 管理重新識別個人身份的資訊風險：流程審核
4. 管理重新識別個人身份的資訊風險：分享細節的規則
5. 管理數據外洩
6. 制定合規框架

詳情載於附錄：詳細建議。

附錄：詳細建議

設有 13 項澳洲私隱準則（Australian Privacy Principles，下文簡稱「APP」）。以上準則屬於管理個人資料相關之《私隱法》（Privacy Act）。每項建議後方備有相關 APP 之清單。APP 詳情載於澳洲資訊委員會辦事處網站之澳洲私隱準則（Australian Privacy Principles）頁面。

建議一：日後將數據集增添至殘障數據資產系統的準則

背景

國家殘障數據資產系統章程（National Disability Data Asset Charter）（簡稱「章程」）對殘障數據資產系統的使用方法設有嚴格準則及規則。殘障社群編撰上述章程。委員會及殘障人士服務部長會批准上述章程。

對數據集增添至殘障數據資產系統的時機設有清晰規則亦同樣重要。數據集是指資料、紀錄及事實的收集處。

擬定方法

Maddocks 建議我們制定一套準則，以指引政府將新數據增添至殘障數據資產系統的方法。我們應於國家殘障數據資產系統網站上發布以上準則，並對加入的數據相應描述。

Maddocks 建議上述準則應至少將下列因素納入考慮：

- 增添全新數據集的公眾利益 - 此類做法的評估方法可能備有指引，例如了解殘障社群是否會受惠
- 殘障數據資產系統的新數據會多有用 - 僅應於獲批的研究項目可能會用上的情況下，方增添至殘障數據資產系統
- 全新數據集的資訊種類及使用的限制，例如是否設有敏感資訊，即使《私隱法》並無將其定義為敏感資訊
- 數據是否包括原住民或其他弱勢社群的資訊。

相關 APP

- APP 1：個人資料開放透明的管理
- APP 3：收集個人資料
- APP 6：使用或披露個人資料
- APP 11：個人資料的安全

建議二：數據服務提供者收集通知書

背景

我們會以各合法途徑將數據增添至殘障數據資產系統內。以上情況視乎數據服務提供者的收集方式。數據服務提供者屬於政府機構，向殘障數據資產系統提供予以列入的數據。部分數據無須獲得他人同意，即可合法地向殘障數據資產系統分享。

重要的私隱準則是確保公眾知道個人資料獲第三方使用及透露的方式。

擬定方法

收集通知書是機構要求獲取公眾個人資料所示的聲明書。上述通知書說明需要相關資料的原因及使用的方法。Maddocks 建議數據服務提供者以標準字眼撰寫收集通知書。例如，以表格形式或於網站上。

委員會應支持此類標準字眼。董事會應批准此類標準字眼。

數據服務提供者應就全新的標準字眼因時更新收集通知書。例如，可能是將標準字眼列入數據分享協議內；或者應該獲得鼓勵而如此行。上述做法是知會公眾個人資料使用方式的最有效方法。

相關 APP

- APP 1：個人資料開放透明的管理
- APP 3：收集個人資料
- APP 5：收集資料通知書

建議三：管理重新識別個人身份的資訊風險：流程審核

背景

草擬章程的一項準則是確保數據以私隱安全的方式保留。數據資產系統僅會包括無法識別個人身份的資訊。但某些人士留意到，外界可能會容易重新識別個人身份的數據，而且這類風險會逐漸增加。

擬定方法

Maddocks 建議委員會設有定期流程，以審查如何管理數據被重新識別的風險。例如，可能是每年執行審查工作。

委員會亦可能決定將會觸發審查工作的情況。例如，如果出現數據外洩事故或政府發布網絡安全威脅的建議。上述舉措旨在確保於移除可識別個人身份的資訊及管理重新識別個人身份的風險期間，我們能不斷套用最佳做法。此類做法將考慮日後會改變的科技及風險。

相關 APP

- APP 6：使用或披露個人資料
- APP 11：個人資料的安全

建議四：管理重新識別個人身份的資訊風險：分享細節的規則

背景

假如殘障數據資產系統內的資訊獲外界重新識別，則很有機會對受影響人士造成較大傷害，而原因是構成殘障數據資產系統的資訊種類，另一個原因是殘障數據資產系統包括弱勢社群的資料。

根據數據管治框架（Data Governance Framework），我們會制定無法識別個人身份資訊之政策。以上框架屬於一套規則，旨在確保公眾以安全穩妥、符合道德操守的合法途徑分享、管理及使用數據。

擬定方法

Maddocks 建議任何無法無法識別個人身份資訊的政策於下列範圍應清晰可見：

- 假如某名人士因使用殘障數據資產系統的資訊令個人身份受外界識別所構成嚴重傷害的風險
- 使用數據期間考慮及管理此類風險的需要。

以上政策亦應包括對使用數據的項目所適用的規則。我們應考慮是否需要更多流程，例如於其他數據集使用的流程。例如，數據分析結果離開基本系統前，檢查相關結果正確移除可識別個人身份的資訊之流程。

相關 APP

- APP 6：使用或披露個人資料
- APP 11：個人資料的安全

建議五：管理數據外洩

背景

政府機構共同合作，以管理殘障數據資產及其基本系統。這表示可能會增加數據外洩事故的風險。對於政府機構而言，亦有更大風險無法迅速處理這類外洩問題。

根據數據管治框架（Data Governance Framework），我們會設立數據外洩回應計劃（Data Breach Response Plan），當中包括紀錄任何數據和私隱外洩事故。上述計劃將涵蓋年度審核。

擬定方法

Maddocks 建議數據外洩回應計劃設有處理政府機構從事數據資產系統工作的方法。上述計劃應清晰說明各個相關政府團體和機構必須擔當的職責，當中包括 ABS 儲存數據的時候。

上述計劃亦應列明負責向下列機構撰寫外洩事故書面通知書的人士：

- 澳洲資訊委員會辦事處（Office of the Australian Information Commissioner）
- 國家數據委員會辦事處（Office of the Australian Information Commissioner）
- 受外洩事故影響的任何人士。

相關 APP

- APP 11：個人資料的安全

建議六：制定合規框架

背景

屆時會落實一系列規則及流程，以管理數據資產系統，當中包括數據分享協議。根據數據管治框架（Data Governance Framework），會有執行基本系統稽核及審查工作的計劃。

擬定方法

Maddocks 建議董事會制定合規框架，以檢查各人是否遵循數據分享協議。上述框架應涵蓋數據資產及其基本系統。例如，使用數據資產及獲批系統的人士可每年向下列機構匯報：

- 國家殘障數據整合基礎建設監護者（Australian National Data Integration Infrastructure Guardian）
- 國家殘障數據資產系統監護者（National Disability Data Asset Guardian）。

以上監護者屬於 ABS 官員，負責以安全合法、符合道德操守的方法管理殘障數據資產及其基本系統，亦會批准存取使用以上系統的人士。

報告可能包括下列方面的檢查工作：

- 收集通知書
- 保安
- 系統及流程的獨立審查等事項。

相關 APP

- APP 1：個人資料開放透明的管理
- APP 6：使用或披露個人資料
- APP 11：個人資料的安全

了解詳情

聯邦合作夥伴已從 2023 年私隱影響評估（PIA）回應了六項建議。2023 年回應 PIA 的內容載於國家殘障數據資產系統網站上的國家殘障數據資產系統私隱頁面（Privacy for the National Disability Data Asset）。