

HRMI資料保護與私隱權政策

作為發展公民和政治權利進步衡量指標的一部分，HRMI須收集個人及敏感資料。以下兩組資料將分開儲存：

1. 個人資料，包括潛在專家調查問卷受訪者及其提名者的姓名及聯絡方式。
2. 我們年度專家調查問卷所收集的問卷回覆（不記名／匿名）。

對於我們所持有的任何與您有關的個人資料，您有權要求我們提供副本；如果您認為該等資料有誤，則有權要求予以更正或永久刪除。如需索取您的資料副本，或希望予以更正或永久刪除，請寄送電郵到survey@humanrightsmeasurement.org與我們聯絡

以下會解釋我們將如何確保上述資料之安全。

1. 潛在問卷回覆者的姓名及聯絡資料

此資料分兩個階段進行收集。首先，參加問卷調查的人權推動者可能會由 HRMI 指派的大使提名（透過安全的網上表格）。這些大使是我們的當地合作夥伴、可信的合作組織人員，在某些情況下，也會是來自現有的調查受訪者。然後，我們將詢問被提名者是否願意參加調查。如果他們答允，他們會透過簽署安全的網上同意書來提供其姓名和電郵地址。我們的安全政策主要有以下特徵：

- 所有網上表格均託管在具有安全通訊協定（SSL）證書並受到 https 保護的 HRMI 網站上。這可以確保資料在傳輸過程中是安全的（加密）。
- 透過同意書提交的姓名和電子郵件將直接（加密）發送至我們的客戶關係管理（CRM）軟體。基於雲端的 CRM 已通過所有相關安全 ISO 標準認證，包括 27001、27017 及 27018，以確保會用加密方式獲取、管理和保留所有資料。讀取 CRM 內資料的權限僅限於紐西蘭 HRMI 團隊中的小部分員工。
- HRMI 會透過此資料向每位潛在調查受訪者發送獨特的連結，以讓其參與 HRMI 網上專家調查問卷調研。
- 被提名參與調查但沒有提交同意書的人員，其姓名將不會加入至 CRM 資料庫中；且每年調查數據發布後，我們將刪除所有被提名者的詳細資料。

2. 問卷調查回覆

該調查會在具有安全通訊協定（SSL）證書並受到 https 保護的 [Qualtrics](#) 網站上進行。這表示所有輸入和傳輸的資料都會經過加密，而且不會儲存連線的 IP 地址。僅限喬治亞大學（UGA）全球問題研究中心（GLOBIS）的 HRMI 工作小組人員有權查看 Qualtrics 所收回的資料。

調查受訪者面臨的主要潛在風險是，如果他們的電郵信箱被駭客入侵或受到監視，敵對間諜可能會看到他們正在與 HRMI 進行通訊，並知悉其可能參與我們的公民和政治權利指標項目。¹ 但這些間諜可能無法讀取其提交的調查資料。唯一的例外是，如果受訪者受到例如鍵盤鍵入記錄這類監視，在該情況下，受訪者在調查中的某些鍵入內容可能會洩露。如果您擔憂此問題，我們強烈建議受訪者使用其有完全控制權限且非共享的信任設備填寫調查問卷，並且遵循其它指南（[在我們網站上有列出](#)）以保護自己免受網上監控。

HRMI 透過 Qualtrics 收到的調查回覆將保密。即我們不會將回覆與調查受訪者個人連結起來。然而，在極少數情況下，所提交的定性回答可能可以用於識別某些受訪者。因此，我們劃定了 3 種不同的資料安全級別，從 1(機密)到 3(公開)。

- 1 - 機密：喬治亞大學 HRMI 工作人員透過 Qualtrics 收到的初始原始資料包括所有受訪者回覆的定性和定量回答。這些資料在處理後將從 Qualtrics 伺服器中刪除。只有受過數據安全培訓和正在進行相關研究的人員才能訪問這些資料。我們最後會將銷毀所有可能識別受訪者身分的資料。
- 2 - 研究數據：完全去識別化的調查回覆(用於研究和計算 HRMI 指標)，因為數據是完全匿名的，因此無需特別關注其安全性。這些數據可作為複製數據於 HRMI 出版物網上共享。
- 3 - 公開：發佈於 HRMI [人權追蹤系統](#)上的匯總數據是 HRMI 指標，可直接從 HRMI 網站下載。

¹ 為了降低這種安全風險，我們提供以下 [資訊](#) 以讓潛在調查受訪者了解如何保護自己免受線上監視。