亞太區私隱機構 科技工作分組

《個人資料匿名化入門指南》

英文版於2025年6月出版
(中文譯本由香港個人資料私隱專員公署以及
澳門個人資料保護局於2025年7月聯合出版)

20250728

個人資料匿名化入門指南

引言

本指南概述基本的匿名化概念及機構可採取的實際步驟，讓機構能夠從具結構、文字性及非複雜數據集着手，開展匿名化工作。本指南旨在讓讀者在參研更高階的資源或其所屬司法管轄區的進一步具體指引（如有）前，對匿名化有基本的了解。

要妥善進行匿名化，需要諳熟資料背景並具備採用匿名化技術的能力。如果資料使用者／負責處理個人資料的實體認為相關匿名化過於複雜或並沒有具備所需技術，應考慮聘請專家進行匿名化。讀者亦應留意，匿名化及再識別技術是不斷發展的研究範疇，而相關方法亦推陳出新。計劃進行匿名化的資料使用者／負責處理個人資料的實體應密切留意相關技術的最新發展或諮詢該領域的專家意見。

我們亦建議資料使用者／負責處理個人資料的實體參考題為《資訊安全、網絡安全及私隱保障 — 加強私隱的資料去識別化框架（ISO/IEC 27559:2022[1]）》的 ISO 標準。該標準指出匿名化不僅涉及資料本身，更涵蓋資料分享及使用的情境及管治常規。採納這些最佳行事常規有助機構在有效管理再識別風險的同時，保持匿名化資料的實用性。

免責聲明：本指南旨在從技術層面探討匿名化，而非從法律或政策層面出發，只作一般參考用途。本指南不構成法律意見，亦不一定反映個別亞太區私隱機構或亞太區私隱機構科技工作分組成員的官方政策或立場。本指南並不意圖提供所有處理匿名化相關問題的方法，亦不

[1] 讀者務必留意，撰寫 ISO/IEC 27559 的一個假設，是在受私隱法律規管的資訊（即「個人」資訊）與不受相關法律規管的資訊（即「匿名化」資訊）有明確的二元區分。雖然往時的私隱法律也是基於同樣的假設實施，但現今的私隱法律則傾向使用更具彈性的三重區分，區分個人資訊、「去識別化」（或「假名化」）資訊及匿名化資訊，而去識別化（或「假名化」）資訊則仍受私隱法律所規管。有鑑於這個差異，在現今私隱監管框架之下，按照 ISO/IEC 27559 而「匿名化」的資訊是否或在甚麼情況下應被視為去識別化（或「假名化」）資訊仍未清晰。

能取代相關司法管轄區的規管指引。機構應參照適用的規管指引（如有的話），以確保符合相關的資料保障規例。

請注意，此《個人資料匿名化入門指南》為 Guide to Getting Started with Anonymisation 英文版本的中文譯本，由香港個人資料私隱專員公署及澳門個人資料保護局編纂，為方便中國香港及澳門兩特別行政區讀者參考之用。如中、英文兩個版本有任何抵觸或不相符之處，應以英文版本為準。此譯本所使用的詞彙並非直接採用《個人資料（私隱）條例》(《私隱條例》) 及《個人資料保護法》中的正式法律用語，亦未必與上述條例所界定的法律定義完全對應。相關詞彙僅供參考，旨在協助讀者理解本指南內容，此譯本並不構成對《私隱條例》及《個人資料保護法》條文的法律詮釋。

何謂匿名化？

從技術層面而言，匿名化[2]是在考慮現今科技水平下，以合理的措施將個人資料（不論單獨使用或與其他資訊結合使用）轉化為無法再用作識別一名個人[3]的資料。

為何要將資料匿名化？

一般而言，經過匿名化處理的資料不會被視為個人資料。然而，我們需認識到《ISO/IEC 27559 — 加強私隱的資料去識別化框架》所概述的匿名化過程需要嚴謹評估、風險管理及持續的管治。此過程包括情境評估、資料評估、可識別度評估及實施穩健的風險緩減措施，以確保再識別風險維持在預設的可承受水平之下。持續監察並遵從既定的匿名化行事常規對於確保匿名化資料維持「非個人化」至關重要。

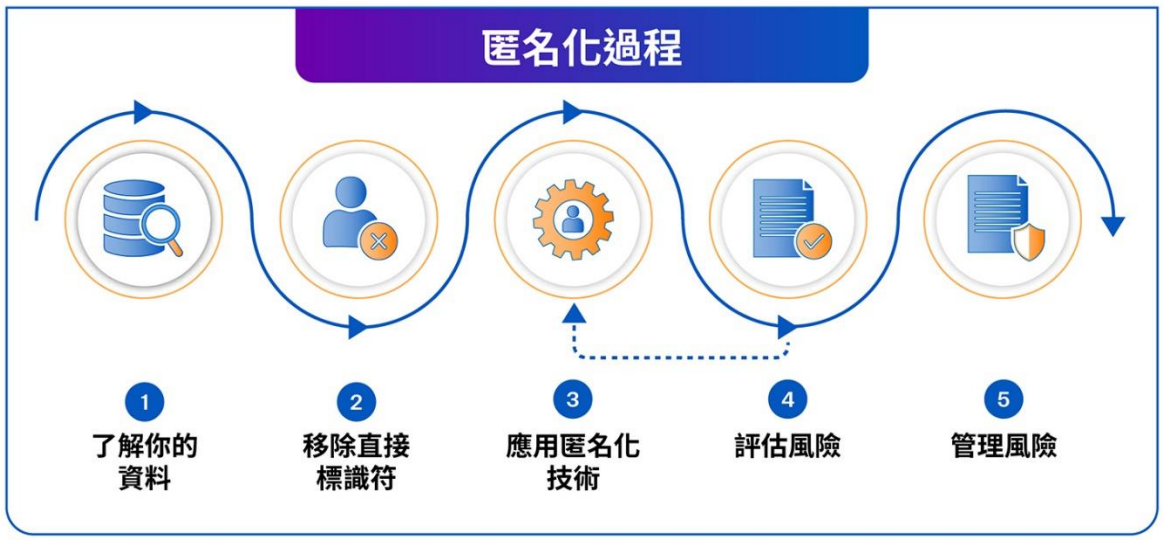
[2] 在某些國家的資料保障法律中，「匿名化」亦可稱為「去識別化」，而某些定義可能認為「去識別化」僅是移除直接標識符。此外，如果資料仍存在風險需要管理，某些司法管轄區可能會視這些資料為「假名化」資料，而非「匿名化」資料。「匿名化」資料及「去識別化」資料的法律標準在不同資料保障司法管轄區可以有差異。

[3] 本文件第 4 步將探討如何評估再識別風險。

最佳行事常規及標準（如 ISO/IEC 27559 中所述）將匿名化視為風險為本的過程，其中包括應用匿名化技術處理資料，以及實施其他私隱及安全措施，以緩減再識別風險[4]。本指南提出切實可行的建議步驟，協助機構在評估及減低這些風險的同時，仍能取得有用的資料。

例如，機構與第三方分享資料時將資料匿名化，機構可從資料中取得有用資料的同時，資料當事人仍得到保障。資料保障法律亦可能要求機構在不再有合理理由保留個人資料時，銷毀個人資料或將其匿名化。

匿名化過程



上圖為本指南建議的匿名化過程之簡化[5]概覽。

第 1 步：了解你的資料

個人資料紀錄由對個人具有不同程度可識別度及敏感度的數據屬性組成。一般而言，匿名化包括移除直接標識符及修改間接標識符。目標屬性通常維持不變。

[4] 本指南第 1 至第 5 步適用於該等司法管轄區內的機構。
[5] 這些步驟並非旨在規範，而是就匿名化過程提供一般性指引。機構可視乎情況及內部程序作出調整，例如在應用匿名化技術前進行風險評估。

直接標識符是一般對個人而言獨一無二的數據屬性，同時可於資料紀錄中作為主要數據屬性，用作重新識別一名人士。直接標識符的常見例子包括姓名及國民身分證號碼。

一般而言，**間接標識符**對個人來說，並非獨一無二的數據屬性，但其組合有可能具有獨特性，當與其他資訊（包括直接標識符）結合時，便可用來重新識別資料紀錄中的個人。間接標識符的常見例子包括出生日期、性別及郵政編號。

目標屬性是指作為數據集主要用途的剩餘數據屬性。就評估是否充分匿名化而言，這項數據屬性可能本質上屬於敏感，一旦被披露，很有可能對個人造成不利影響。這些數據屬性通常是不公開或不易於取得。其中一個目標屬性的例子是個人的健康診斷。當這些目標屬性可以被輕易取得或以其他方式查閱，處理時必須格外小心，並應將這些數據屬性分類為間接數據屬性。

第2步：移除直接標識符

移除所有直接標識符。如有需要，應為每個紀錄編配一個假名。每個直接標識符的假名都應是獨特的。假名的編配應是穩妥的，即它們不應包含可識別的資訊，亦不應被未經授權者透過猜測或運算原有直接標識符的數值來還原相關資訊。

第3步：應用匿名化技術

這個步驟是關於應用匿名化技術至間接標識符，使間接標識符無法與其他可能載有額外資訊的數據集結合，以重新識別個人。讀者應留意，應用這些技術將會修改間接標識符的數據數值，並可能影響匿名化資料的效用。匿名化技術包括資料壓制、資料遮蓋、資料泛化、在資料中加入雜訊、資料抽樣及資料交換。ISO/IEC 20889 題為《加強私隱

的資料去識別化術語及技術分類》的標準已詳列各項可行的匿名化技術，以供參考。

選擇適用於數據集及資料使用方式的技術十分重要。機構有責任確保所選擇的技術適合相關的情況。就私隱及資料效用而言，不同技術各有優劣，機構應了解這些利弊，以便在知情的情況下慎重選擇將要使用的技術。

第 4 步：評估再識別風險

計算匿名化資料的再識別風險至關重要。*k*-匿名性（k-anonymity）[6]等方法可用於計算再識別風險，但*k*-匿名性未必適用於所有數據集。機構亦可考慮使用特別獨特偵測演算法（Special Unique Detection Algorithms，SUDA）及μ-Argus等其他方法或工具評估共享數據集的再識別風險。

k-匿名性是計算數據集的再識別風險的簡單方法，可用於那些非複雜且沒有大量數據屬性的數據集。基本上，*k*-匿名性指的是若數據集內的相同紀錄歸類成同一組時，各個組別中最少的項目數量。評估數據集整體再識別風險時，項目最少的組別通常用來代表最差情況。一般而言，*k*-匿名性計算只考慮間接標識符。*k*-匿名性數值愈高，代表再識別風險愈低；*k*-匿名性數值愈低，則表示再識別風險愈高。以下圖1為一個簡單的例子，列出具有三組相同紀錄的數據集，每組的*k*數值介乎2至4不等。整體而言，這個數據集的*k*-匿名性數值為2，反映整個數據集內的最低數值（即最高風險）[7]。

[6] 一般而言，匿名化是否充分乃按個案逐一評估。新加坡個人資料保護委員會建議 *k* 數值最少要達到 5，再加上相關保護措施，才算充分匿名化。此外，*k*-匿名性主要用於防止鏈結攻擊(linking attack)及單獨攻擊(singling attack)，如欲防止推理攻擊(inference attack)等其他攻擊可考慮採用 *k*-匿名性的延伸，例如 *l*-多樣性(*l-diversity*)及 *t*-相近性(*t-closeness*)。

[7] 專注於最高風險是一種較為保守的風險策略，即考慮數據集內最高再識別風險。此外還有平均風險及精確平均風險等其他策略。

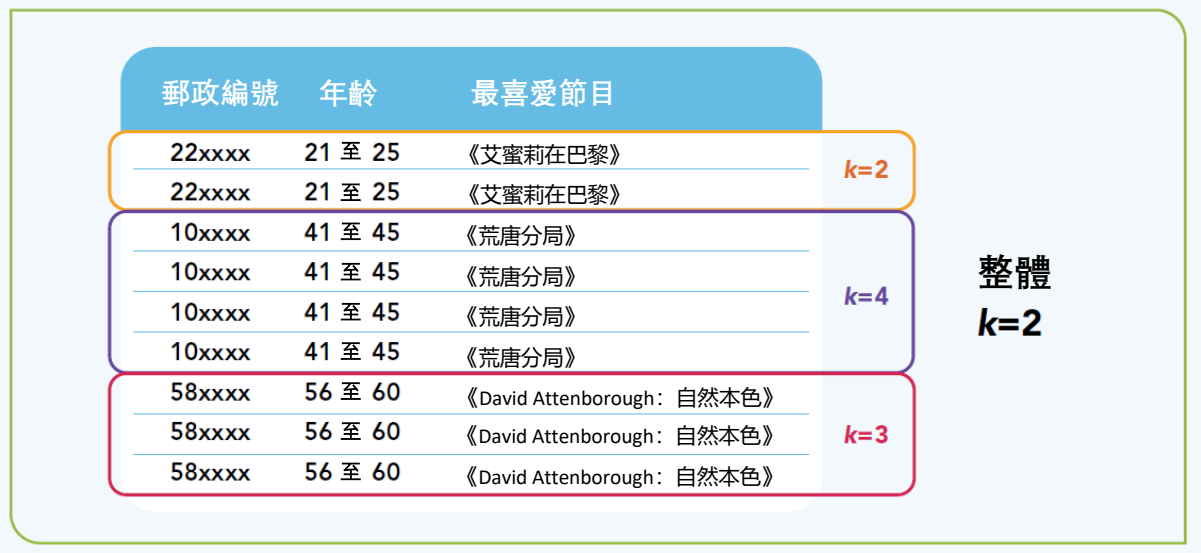


圖 1：*k*-匿名性的示意圖

進行「有動機的入侵者」測試(motivated intruder test)[8]可以評估應用匿名化技術後的再識別剩餘風險。此測試評估的是特定人士是否能從匿名化資料中重新識別個人，該類人士是指有動機、具合理能力、可存取公共或私人可連結數據或資訊（例如互聯網、商用數據集及公共目錄等公開資訊），並採用標準偵查技術（例如干擾及數據連結）的人士。

機構應基於再識別風險評估的結果，確保其資料已充分匿名化。機構可能需要調整其技術、採取額外措施、修改數據集的範圍、移除離群值等。因此，機構可能需要返回第 3 步或更早步驟，並重複此循環，直至第 4 步的結果符合要求，即資料已充分匿名化。

第 5 步：管理再識別風險

緩減措施旨在管理應用匿名化技術處理資料後的任何剩餘風險。一般而言，有較高剩餘風險（例如 *k*-匿名性數值較低）的匿名化資料需要較強的緩減措施。機構在決定採取哪種緩減措施時，亦應考慮再識別可能對個人造成的損害。

[8] 於英國資訊專員辦公室發布的實務守則《匿名化：管理資料保障風險的實務守則》中重點闡述。

緩減措施一般包括用作確保只有獲授權用戶才能查閱共用的匿名化資料的安全措施，以及確保資料只用於原定用途的法律及／或管治措施。

如果資料使用者／負責處理個人資料的實體選擇保留與匿名化資料相關的身分對應或身分連結資訊，應採取緩減措施，以確保該些資訊的安全性。

雖然應用緩減措施可被視為匿名化技術，但亦可被視為資料保障或私隱法律的延伸。如果在第 4 步後，再識別風險仍未能降低至可將資料視為匿名化的水平，該資料將仍被視為可識別個人身分，而資料保障或私隱法律則繼續適用於這些資料。在某些司法管轄區，應用緩減措施會被視為將資料假名化的條件，而非匿名化；與此同時，其他司法管轄區可能會將應用相同措施視作為匿名化而採取的風險為本策略的一部分。有關這方面的分類，機構應參考相應司法管轄區的規例。

ISO/IEC 27559 內的實用建議

除上述五個步驟外，機構亦可參考 ISO/IEC 27559 就情境評估、資料評估、可識別度評估及可識別度緩減措施，以及管治所提供的實用框架及建議。

情境評估：評估提供資料給資料接收方的環境及情況（包括威脅模型 (threat modelling)）、保安及私隱行事方式，以及再識別的動機及能力。

資料評估：了解資料的特色，並構建可利用漏洞的潛在攻擊模型，包括資料特色、攻擊模型，以及選擇用作量化可識別度的資料私隱模型。

可識別度評估及緩減措施：評估遭受攻擊的機率及成功重新識別資料當事人的可能性。此框架列出量化可識別度的方法，並建議緩減措施，例如重新設定環境或將資料改頭換面以減低可識別度。

去識別化／匿名化管治：管治包括建立原則、政策及程序，以管理資料處理活動，並確保遵從資料安全及私隱標準，亦涵蓋角色及責任、監管風險及處理意外的披露。

其他建議行事方式

機構應作定期檢視，以確保再識別風險一直維持在低水平，亦需確保沒有新科技及技術的出現，或沒有新的數據集可供存取或可供公眾查閱，從而令匿名化資料被重新識別。定期檢視亦可確保風險緩減措施有效並能如預期般運作，且在機構的情況有變時仍是合適的。

一般而言，資料保障機構是否視一組資料為匿名化，取決於重新識別的可能性。視乎司法管轄區而定，資料保障機構亦可考慮機構所採用的保護措施（包括技術、管治及合約措施）及匿名化程序。因此，在進行匿名化時保存此類資訊的紀錄也是有用的。

附件 A：與匿名化有關的資源

國際標準化組織 (International Organization for Standardization) (ISO) ／國際電工委員會 (International Electrotechnical Commission) (IEC)

國際標準化組織／國際電工委員會發布了包括以下項目在內，與匿名化有關的標準。

資源	描述
《ISO/IEC 20889:2018 — 加強私隱的資料去識別化術語及技術分類》	此項標準闡明了術語、去識別化技術的分類（按照資料的特色而定），以及它們對減低再識別風險的適用性。 請參閱：※只有英文版 https://www.iso.org/standard/69373.html
《ISO/IEC 27559:2022 — 資訊安全、網絡安全及私隱保障 — 加強私隱的資料去識別化框架》	此項標準提供了一個框架，用作識別及緩減再識別風險及與去識別化資料的生命周期有關的風險，有助機構在實際操作中決定如何實施去識別化程序。此標準基於最佳行事方式和採取風險為本的策略，並以通用性為基礎，務求獲廣泛採用。 請參閱：※只有英文版 https://www.iso.org/standard/71677.html

澳洲（聯邦）

澳洲資訊專員辦公室就澳洲國家私隱法律下的去識別化提供指引。根據《1988 年私隱法》（聯邦），為確保資訊「去識別化」，實體必須採用類似於「匿名化」的方法。

由澳洲資訊專員辦公室和澳洲聯邦科學與工業研究組織轄下的 Data61 共同發布的《去識別化決策框架》旨在協助機構有效地進行資料去識別化。《去識別化決策框架》是一份實用易明的指引，協助澳洲機構在處理個人資料並考慮分享或發布個人資訊的同時，履行其道德責任和法律義務。

此外，澳洲資訊專員辦公室就《去識別化與私隱法》提供了指引，其中包括去識別化和保障私隱的一般建議，以在保障私隱的同時最大限度地發揮資料的效用和價值。

資源	請參閱
《去識別化決策框架》	※只有英文版 https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/de-identification-decision-making-framework
《去識別化與私隱法》	※只有英文版 https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/de-identification-and-the-privacy-act

澳洲維多利亞省

澳洲維多利亞省資訊專員辦公室於其網站提供一系列免費資源，涵蓋以下項目：

- 去識別化的入門級簡介—去識別化的意義、運作方式，以及當中涉及的風險及挑戰；
- 實務建議— 資訊去識別化時應考慮的事項，以及如何管理再識別風險；及
- 較深入的去識別化指引— 去識別化的技術，以及將這些技術用於保障單位紀錄層面的個人資訊的限制。

在澳洲維多利亞省資訊專員辦公室行使其司法管轄區權時，「去識別化」一詞用於形容本指南所定義的「匿名化」。

資源	請參閱
《去識別化簡介》	※只有英文版 https://ovic.vic.gov.au/privacy/resources-for-organisations/an-introduction-to-de-identification/
《去識別化：風險管理的措施》	※只有英文版 https://vimeo.com/722443647
《去識別化的限制》	※只有英文版 https://ovic.vic.gov.au/privacy/resources-for-organisations/the-limitations-of-de-identification-protecting-unit-record-level-personal-information/

韓國

韓國個人資料保護委員會在其於 2022 年修訂的《假名化資料處理指引》中解釋假名化資料管治的情況。

韓國《個人資料保護法》規定假名化資料為個人資料。韓國個人資料保護委員會發布了上述指引以讓公眾更加了解假名化資料的處理、組合、輸出及安全措施。

該指引詳列處理假名化資料過程中每個步驟的注意事項，以及如何透過技術、行政及實體安全措施保障資料當事人的權利。

此外，人工智能科技發展令圖像及影片等非結構化數據的使用需求日增，為回應需求，韓國個人資料保護委員會於2024年2月發布指引，內容涵蓋醫療、交通及聊天機械人等不同領域的詳盡個案及情境。

資源	請參閱
假名化的概述	※只有英文版 https://www.pipc.go.kr/eng/user/lgp/bnp/pseudonymization.do
假名化非結構化數據的指引（PDF 檔案; 英文節略版）	※只有英文版 https://www.pipc.go.kr/eng/user/lgp/law/ordinancesDetail.do?bbsId=BBSMSTR_000000000005&nttId=2699#none
假名化資料處理指引（2022 年版）	※只有韓文版 https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=G010030000&nttId=8000

日本

日本個人情報保護委員會發布了有關《個人情報保護法》下處理匿名化個人資料的指引，支持機構妥善及有效地實施保障個人資料的措施。日本個人情報保護委員會繼而發布一份載有處理匿名化個人資料更多細節的報告，以促進機構自我規管。這些文件同時就假名化個人資料作出說明，而根據日本《個人情報保護法》的規定，假名化個人資料與匿名化個人資料兩者性質不同。

資源	請參閱
指引	※只有日文版 https://www.ppc.go.jp/personalinfo/legal/#anc_Guide
個人情報保護委員會秘書處的報告	（關於法律制度的版本）※只有日文版 https://www.ppc.go.jp/files/pdf/report_office_seido2205.pdf （關於個案研究的版本）※只有日文版 https://www.ppc.go.jp/files/pdf/report_office_zirei2205.pdf

新加坡

新加坡個人資料保護委員會發布了建議指引闡釋《個人資料保護法》下匿名化的定義及資料要符合哪些條件才會被視為匿名化。新加坡個人資料保護委員會亦發布了一份有關匿名化的技術指引，就實施匿名化提供建議。最後，資料匿名化工具是一項與技術指引相輔相成的免費工具，有助讀者學習匿名化及對簡單的數據集進行匿名化。

資源	請參閱
《有關個別專題的個人資料保護法建議指引》（第 3 章 — 匿名化）	※只有英文版 https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/ag-on-selected-topics/advisory-guidelines-on-the-pdpa-for-selected-topics-(revised-may-2024).pdf
• 《基本匿名化指引》 • 資料匿名化工具	英文版： https://www.pdpc.gov.sg/Help-and-Resources/2018/01/Basic-Anonymisation 西班牙文版（由西班牙資料保障機構發布）： https://www.aepd.es/es/documento/guia-basica-anonimizacion.pdf https://www.aepd.es/es/descargas/herramienta-anonimizacion-pdpc
[影片] 簡介個人資料保護委員會的資料匿名化工具	※只有英文版 www.youtube.com/watch?v=qlnYRl5VwQQ

附件 **B**：個案研究

本部分提供一個假設性例子說明上述步驟。

在本例子中，一間名為 Vivogym 的健身室希望與行銷伙伴 The Pink Group 分享匿名化資料以彙編其客戶的個人概況並設立全新行銷活動。

下表摘錄自 Vivogym 數據庫的原始客戶資料。此例中所有資料均屬虛構。以下列出 10 項來自數據集的紀錄。

序列	姓名	出生日期	郵政編號（新加坡）	體重（公斤）	身高（米）	過去 6 個月使用時間最多的項目
1	Demond Nix	9/12/1996	322607	52	1.60	跑步機
2	Treyvon Coker	24/12/1998	335662	56	1.75	普拉提
3	Jarred Zielinski	3/10/1995	355895	72	1.65	游泳
4	Rolando Toth	10/12/1996	359383	79	1.67	健身單車
5	Benny Beckman	8/12/1996	316551	65	1.60	舉重
6	Dakota Birch	5/9/1997	326125	66	1.75	舉重
7	Jacques Colburn	4/9/1995	339035	72	1.68	自由搏擊
8	Kendyl Fletcher	25/10/1999	346214	79	1.72	舉重
9	Keegan Knapp	26/10/1997	346204	59	1.62	普拉提

10	Yoselin Provost	4/9/1995	324946	61	1.75	舉重
（篇幅所限其他紀錄未能盡錄）						

第 1 步：了解你的資料

在本例子中，Vivogym 按以下方式分類數據屬性：

數據屬性	姓名	出生日期	郵政編號（新加坡）	體重（公斤）	身高（米）	過去 6 個月使用時間最多的項目
分類	直接標識符	間接標識符	間接標識符	間接標識符	間接標識符	目標屬性

第 2 步：移除直接標識符

在本例子中，唯一的直接標識符是客戶的姓名。該項資料已從數據集中移除。

序列	~~姓名~~	出生日期	郵政編號（新加坡）	體重（公斤）	身高（米）	過去 6 個月使用時間最多的項目
1	~~Demond Nix~~	9/12/1996	322607	52	1.60	跑步機
2	~~Treyvon Coker~~	24/12/1998	335662	56	1.75	普拉提
3	~~Jarred Zielinski~~	3/10/1995	355895	72	1.65	游泳
4	~~Rolando Toth~~	10/12/1996	359383	79	1.67	健身單車
5	~~Benny Beckman~~	8/12/1996	316551	65	1.60	舉重

6	~~Dakota Birch~~	5/9/1997	326125	66	1.75	舉重
7	~~Jacques Colburn~~	4/9/1995	339035	72	1.68	自由搏擊
8	~~Kendyl Fletcher~~	25/10/1999	346214	79	1.72	舉重
9	~~Keegan Knapp~~	26/10/1997	346204	59	1.62	普拉提
10	~~Yoselin Provost~~	4/9/1995	324946	61	1.75	舉重
（篇幅所限其他紀錄未能盡錄）						

第 3 步：應用匿名化技術

健身室決定如何將不同的間接標識符匿名化，方法詳述如下：

間接標識符	匿名化技術
出生日期	由確實日期省略至只有出生年份。
郵政編號（新加坡）	遮蓋 6 位郵政編號的最後 4 位數字。這將由原本可能指示出個別住宅單位改為較粗略的地區格式。
體重（公斤）	將體重及身高合併為身體質量指數（BMI），然後將指數歸納為以 10 為單位的數值範圍。
身高（米）	

匿名化後的數據集將如下顯示：

序列	出生日期	郵政編號（新加坡）	BMI	過去 6 個月使用時間最多的項目
1	1996	32****	20 - 29	跑步機
2	1998	33****	10 - 19	普拉提
3	1995	35****	20 - 29	游泳
4	1996	35****	20 - 29	健身單車
5	1996	31****	20 - 29	舉重

6	1997	32****	20 - 29	舉重
7	1995	33****	20 - 29	自由搏擊
8	1999	34****	20 - 29	舉重
9	1997	34****	20 - 29	普拉提
10	1995	32****	10 - 19	舉重
（篇幅所限其他紀錄未能盡錄）				

第 4 步：評估再識別風險

健身室隨後將數據集內類似的紀錄分組，即擁有相同出生日期、郵政編號及 BMI 的紀錄歸為一組。評估紀錄是否相似時，毋須考慮「過去 6 個月使用時間最多的項目」這項數據屬性，這項數據屬性被分類為目標屬性，而且不會用於 *k*-匿名性運算。

序列	出生日期	郵政編號（新加坡）	BMI	數據集內擁有相同間接標識符的紀錄數目（出生日期、郵政編號及 BMI），即 k	過去 6 個月使用時間最多的項目
1	1996	32****	20 - 29	5	（沒有改變的數值）
2	1998	33****	10 - 19	6	（沒有改變的數值）
3	1995	35****	20 - 29	5	（沒有改變的數值）
4	1996	35****	20 - 29	5	（沒有改變的數值）
5	1996	31****	20 - 29	6	（沒有改變的數值）

6	1997	32****	20 - 29	7	（沒有改變的數值）
7	1995	33****	20 - 29	5	（沒有改變的數值）
8	1999	34****	20 - 29	4	（沒有改變的數值）
9	1997	34****	20 - 29	6	（沒有改變的數值）
10	1995	32****	10 - 19	5	（沒有改變的數值）
（篇幅所限其他紀錄未能盡錄）					

k-匿名性數值可透過專門工具[9]計算，或利用試算表軟件並計算擁有相同間接標識符的紀錄數目。

在本例子中，數據集的整體 *k*-匿名性數值起初為 4，反映整個數據集內擁有最小 *k* 數值（最高風險）的紀錄組別。如果健身室決定改善整體 *k* 數值至 5，可以考慮移除離群值紀錄（標註為紅色的項目，*k* 數值小於 5）以將 *k*-匿名性數值由 4 提升至 5。

健身室進行「有動機的入侵者」測試以評估紀錄的再識別風險，從而評估將匿名化資料進行再識別的可能性。健身室同時亦要考慮如發生再識別時可能對個人構成的任何潛在損害，以及其營運地點所屬司法管轄區的指引。依照上述所言，健身室將重複第 3 至第 4 步，直至 *k*-匿名化數值達至合理的高水平，並同時讓數據集可以發揮其作用（彙編客戶個人概況）。

第 5 步：管理再識別風險

[9] 市面上有多個免費及供商業用途的匿名化工具。

健身室實施以下保護措施以確保任何再識別剩餘風險已經緩減或合理地減至最小：

- 合約式保護措施：與行銷公司簽訂的合約中：
    - 限制匿名化資料僅可用於預期目的及只供預期員工使用；
    - 禁止蓄意嘗試再識別；及
    - 要求在達成預期目的後或不再使用資料時，刪除匿名化資料。
- 技術保護措施：
    - 於行銷公司實施存取控制，控制及限制只供獲授權員工存取匿名化數據集；及
    - 使用資料後刪除匿名化資料，此舉可以事前訂下時間進行。
- 管治保護措施：
    - 保留匿名化數據集的紀錄及匿名化過程的詳情，以及分享資料活動的紀錄。

鳴謝

本指南由亞太區私隱機構科技工作分組成員編撰，分組成員包括：

澳洲維多利亞省資訊專員辦公室
加拿大私隱專員公署
加拿大英屬哥倫比亞省資訊及私隱專員公署
中國香港個人資料私隱專員公署
中國澳門個人資料保護局
日本個人情報保護委員會
新西蘭私隱專員公署
新加坡個人資料保護委員會
韓國個人資料保護委員會

亞太區私隱機構 科技工作分組
英文版於 **2025** 年 **6** 月出版
中文譯本由香港個人資料私隱專員公署以及澳門個人資料保護局於 **2025** 年 **7** 月聯合出版