I809704

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I809704 B**

(45)公告日： 中華民國 112 (2023) 年 07 月 21 日

(21)申請案號：111104689 (22)申請日： 中華民國 111 (2022) 年 02 月 09 日

(51)Int. Cl.： ***G06F16/20 (2019.01)*** ***G06F21/60 (2013.01)***

(30)優先權：2021/02/09 歐洲專利局 21155892.9

(71)申請人：瑞典商安訊士有限公司 (瑞典) AXIS AB (SE)
瑞典

(72)發明人：福克 丹尼爾 FALK, DANIEL (SE)；托雷斯 拉爾夫 伯格 TORRES, RALPH BERGER (SE)

(74)代理人：陳長文

(56)參考文獻：

TW	M597905U	TW	201714113A
TW	202040385A	CN	110494842A
CN	112272828A	US	2019/0377900A1
US	2020/0042685A1	US	2020/0311303A1

審查人員：吳家豪

申請專利範圍項數：15 項 圖式數：5 共 39 頁

(54)名稱

用於安全儲存含有個人資料之媒體及消除所儲存個人資料之裝置及方法

(57)摘要

一種用於儲存含有個人資料之一檔案之方法包括：

獲得一人之一臨時匿名識別符(AnonID.m)，該臨時匿名識別符(AnonID.m)取決於該檔案之一符記(FileID.m)；

從該檔案提取與該人相關聯之個人資料項目；

針對各個人資料項目，產生容許將該個人資料項目恢復至該檔案中的一定位符(Loc.m.n)及該人之一項目特定匿名識別符(AnonID.m.n)，其中藉由將一預定義單向函數應用於該臨時匿名識別符(AnonID.m)及該個人資料項目之一識別符(n)之一組合來產生該項目特定匿名識別符；

將各個人資料項目與該定位符及該項目特定匿名識別符一起儲存在一第一記憶體(421)中；及

將不具有該等個人資料項目之該檔案之一匿名化版本儲存在一第二記憶體(422)中。

A method for storing a file containing personal data comprises:

obtaining a temporary anonymous identifier (AnonID.m) of a person, which temporary anonymous identifier (AnonID.m) is dependent on a token (FileID.m) of the file;

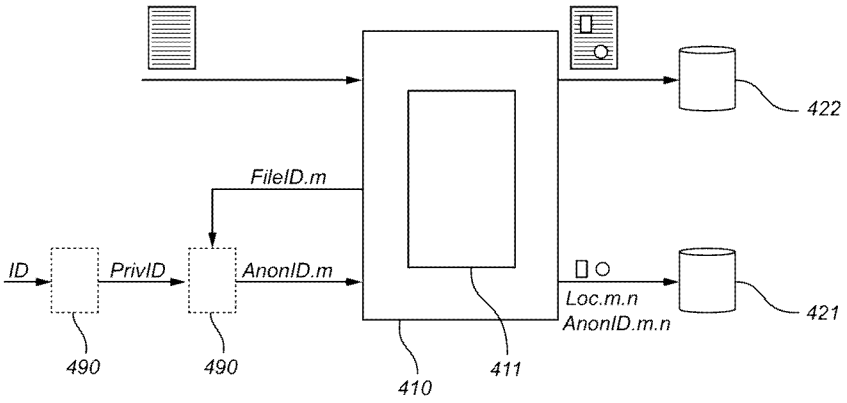
from the file, extracting personal data items associated with the person;

for each personal data item, generating a locator (Loc.m.n), which allows the personal data item to be reinstated into the file, and an item-specific anonymous identifier (AnonID.m.n) of the person, wherein the item-specific anonymous identifier is generated by applying a predefined one-way function to a combination of the temporary anonymous identifier (AnonID.m) and an identifier (n) of the personal data item;

storing each personal data item together with the locator and the item-specific anonymous identifier in a first memory (421); and

storing an anonymized version of the file without the personal data items in a second memory (422).

指定代表圖：



【圖4】

符號簡單說明：

410:裝置

411:處理電路

421:第一記憶體

422:第二記憶體

490:單向函數介面

公告本

I809704

【發明摘要】

【中文發明名稱】

用於安全儲存含有個人資料之媒體及消除所儲存個人資料之裝置及方法

【英文發明名稱】

DEVICES AND METHODS FOR SAFE STORAGE OF MEDIA CONTAINING PERSONAL DATA AND ERASURE OF STORED PERSONAL DATA

【中文】

一種用於儲存含有個人資料之一檔案之方法包括：

獲得一人之一臨時匿名識別符(AnonID.m)，該臨時匿名識別符(AnonID.m)取決於該檔案之一符記(FileID.m)；

從該檔案提取與該人相關聯之個人資料項目；

針對各個人資料項目，產生容許將該個人資料項目恢復至該檔案中的一定位符(Loc.m.n)及該人之一項目特定匿名識別符(AnonID.m.n)，其中藉由將一預定義單向函數應用於該臨時匿名識別符(AnonID.m)及該個人資料項目之一識別符(n)之一組合來產生該項目特定匿名識別符；

將各個人資料項目與該定位符及該項目特定匿名識別符一起儲存在一第一記憶體(421)中；及

將不具有該等個人資料項目之該檔案之一匿名化版本儲存在一第二記憶體(422)中。

【英文】

A method for storing a file containing personal data comprises:

obtaining a temporary anonymous identifier (AnonID.m) of a person, which temporary anonymous identifier (AnonID.m) is dependent on a token (FileID.m) of the file;

from the file, extracting personal data items associated with the person;

for each personal data item, generating a locator (Loc.m.n), which allows the personal data item to be reinstated into the file, and an item-specific anonymous identifier (AnonID.m.n) of the person, wherein the item-specific anonymous identifier is generated by applying a predefined one-way function to a combination of the temporary anonymous identifier (AnonID.m) and an identifier (n) of the personal data item;

storing each personal data item together with the locator and the item-specific anonymous identifier in a first memory (421); and

storing an anonymized version of the file without the personal data items in a second memory (422).

【指定代表圖】

圖4

【代表圖之符號簡單說明】

410: 裝置

411: 處理電路

421: 第一記憶體

422: 第二記憶體

490: 單向函數介面

【發明說明書】

【中文發明名稱】

用於安全儲存含有個人資料之媒體及消除所儲存個人資料之裝置及方法

【英文發明名稱】

DEVICES AND METHODS FOR SAFE STORAGE OF MEDIA CONTAINING PERSONAL DATA AND ERASURE OF STORED PERSONAL DATA

【技術領域】

【0001】 本發明係關於用於安全儲存及再生含有個人資料之媒體及根據請求可靠消除此個人資料之技術。

【先前技術】

【0002】 本發明解決含有個人資料及其他資料之一混合物之媒體之儲存，且特別致力於提出滿足法律文書中規定之特徵之隱私保障措施之此技術，諸如關於在個人資料之處理及此資料之自由移動方面保護自然人之條例(EU) 2016/679 (通用資料保護條例，GDPR)、中國網路安全法、加利福尼亞消費者隱私法及其他美國聯邦及州法律。根據GDPR，各人應具有在任何時間請求完全刪除其儲存之個人資料之一權利。此被稱為資料主體之消除權或「被遺忘權」。然而，在現有技術中，被遺忘權可能與資料版本控制不相容，該資料版本控制係用於在一延長時間內管理大型資料集之一幾乎不可或缺之工具。

【0003】 出現與諸如文本、影像及視訊資料之非離散媒體之儲存有關之一特定複雜性。在一個場景中，先前已同意一公司(資料接收者)儲存

其出現在圖框中之一小部分中之一視訊之一人(資料主體)聯繫資料接收者以請求刪除其個人資料。雖然資料接收者原則上有權保留除該人出現之圖框以外之全部圖框，但從一資料保護角度而言，針對各視訊圖框儲存個人識別符將為非常成問題的。此係因為所識別個人資料之儲存(具有較高相關聯私隱風險)將需要技術配置以確保一較高安全等級，此實際上可為難處理的。因此，為了滿足該人之消除請求，資料接收者可選擇盲目刪除完整視訊序列，此表示有用資料之大量及不當丟失。

【發明內容】

【0004】 本發明之一個目標係使用於儲存含有個人資料之一檔案之方法及裝置可用，以使一資料主體對消除其個人資料之請求可在不必刪除該檔案中含有之其他資料的情況下實行。另一目標係確保安全儲存具有個人資料之檔案，直至提出此一消除請求，但以使其適合於高效管理及處理之一形式。待由本發明解決之一特定安全態樣係防止獲得對所儲存個人資料之未經授權存取之一方識別其所屬之資料主體(人)。一特定效率態樣係容許版本控制。本發明之另一目標係使用於使用本文中提出之技術高效重建具有已經歷安全儲存之個人資料之一檔案之方法及裝置可用。

【0005】 此等及其他態樣由本發明根據獨立技術方案來達成。附屬技術方案係關於本發明之有利實施例。

【0006】 在本發明之一第一態樣中，提供一種用於儲存含有個人資料之一檔案之方法，該方法包括：獲得一人之一臨時匿名識別符(AnonID.m)，該臨時匿名識別符(AnonID.m)取決於該檔案之一符記(FileID.m)；從該檔案提取與該人相關聯之個人資料項目；針對各個人資料項目，產生容許將該個人資料項目恢復至該檔案中的一定位符

(Loc.m.n)及該人之一項目特定匿名識別符(AnonID.m.n)，其中藉由將一預定義單向函數應用於該臨時匿名識別符(AnonID.m)及該個人資料項目之一識別符(n)之一組合來產生該項目特定匿名識別符；將各個人資料項目以及該定位符及該項目特定匿名識別符儲存在一第一記憶體中；及將不具有該等個人資料項目之該檔案之一匿名化版本儲存在一第二記憶體中。

【0007】 由於使用一單向函數產生該等項目特定匿名識別符，所以獲得對該第一記憶體之未經授權存取之一方無法容易地將該等所儲存個人資料項目歸因於該人。該未經授權方亦無法收集與該同一人相關聯之全部個人資料項目。此可被視為該檔案之一假名化形式。由於該檔案在儲存在該第二記憶體中之前匿名化，所以此記憶體可經受不如該第一記憶體嚴格之安全要求。由於該人由一臨時匿名識別符識別，所以該資料接收者可在不要求該人共用其自身之一非匿名識別符的情況下實行用於儲存該檔案之該方法。最後，由於各個人資料項目與該項目特定匿名識別符一起儲存，所以根據請求詳盡且精確地刪除與一特定人有關之全部項目係可能的。

【0008】 在一第二態樣中，提供一種用於從一第一記憶體消除與一人相關聯之個人資料之方法，該第一記憶體儲存個人資料項目以及與該等個人資料項目相關聯之人之對應定位符(Loc.m.n)及項目特定匿名識別符(AnonID.m.n)，該方法包括：獲得該人之一私密識別符(PrivID)；獲得可已從中提取該等個人資料項目之全部檔案之符記(FileID.m)；針對該等檔案之各者，獲得與該人相關聯且可已從該檔案提取的全部個人資料項目之識別符(n)；藉由將一預定義單向函數應用於該所獲得私密識別符(PrivID)及該等所獲得檔案符記(FileID.m)之組合來產生該人之臨時匿名識別符(AnonID.m)；針對該人之各所產生臨時匿名識別符(AnonID.m)，藉由將

該預定義單向函數應用於該臨時匿名識別符(AnonID.m)及該等個人資料項目之該等所獲得識別符(n)之組合來產生該人之項目特定匿名識別符(AnonID.m.n)；及從該第一記憶體消除匹配該人之該等所產生項目特定匿名識別符(AnonID.m.n)之任何者之全部個人資料項目。

【0009】 各個人資料項目與該項目特定匿名識別符一起儲存之事實使得可詳盡且精確地定位及消除與一特定人有關之全部項目。根據該第二態樣之該消除方法無需修改或刪除已從中提取該等個人資料項目之該等檔案之任何匿名化版本。此使該資料接收者自由決定在消除該人之個人資料項目之後如何以及在多大程度上救回該檔案。該資料接收者可根據適合於所關注資料類型之粒度程度及手頭之使用案例來決定在該消除之後重建及使用該檔案之一子集。舉幾個實例，在從一影像消除一人之臉之後，可保留該影像之一裁剪版本以供進一步使用；在從一視訊序列中之某些圖框消除一人之臉之後，可保留全部剩餘視訊圖框或各至少N個剩餘圖框之連續視訊子序列；在從一資料庫列消除一人之姓名之後，可保留該資料庫之其他列；在從一文件消除一人之認證之後，可保留該文件之其他區段等。該消除方法本身不會對該檔案之該救回帶來任何顯著技術限制。最後，為了驗證此方法之一執行已完全消除與該人相關聯之全部個人資料，建立該等所產生項目特定匿名識別符皆不匹配仍儲存在該第一記憶體中之該等個人資料項目之任何者係足夠的。

【0010】 在一第三態樣中，提供一種用於將個人資料恢復至一檔案中之方法，該方法包括：從儲存已從檔案提取之個人資料項目以及與該等個人資料項目相關聯之人之對應定位符(Loc.m.n)及項目特定匿名識別符(AnonID.m.n)之一第一記憶體檢索已從該檔案提取之該等個人資料項目

及對應定位符；從一第二記憶體檢索不具有該等個人資料項目之該檔案之一匿名化版本；及根據該等對應定位符將該等個人資料項目恢復至該匿名化版本中。

【0011】 由於該等個人資料項目與對應定位符及項目特定匿名識別符一起儲存，所以可正確地將該等個人資料項目恢復至該檔案之該匿名化版本中，而不危及與此相關聯之該等人之私密性。該恢復方法可由該資料接收者實行，而無需該人共用其自身之一非匿名識別符。此外，由於該恢復方法使用該檔案之該匿名化版本作為輸入，所以即使當該等個人資料之一些或全部已從該第一記憶體消除時(例如，根據該相關聯人之請求)，該方法仍將穩健地執行。在該情況中，更精確地，該方法可穩健地實施，使得其終止以傳回一可用(一致、可讀、可編輯等)檔案版本，在該檔案版本上，該等經消除個人資料項目之經消除部分不具有破壞效應。

【0012】 當一起使用時，本發明之該三個態樣藉由設計形成具有私密性之一資料儲存生態系統。

【0013】 進一步提供一種裝置，其通信地連接至第一記憶體及第二記憶體且包括經配置以執行該第一態樣、該第二態樣或該第三態樣之該方法之處理電路。再者，本發明係關於一種電腦程式，其含有用於使一電腦或特定言之此裝置實行該第一態樣、該第二態樣或該第三態樣之該方法之指令。該電腦程式可經儲存或分佈在一資料載體上。如本文中使用，一「資料載體」可為諸如經調變電磁波或光波之一暫時性資料載體或一非暫時性資料載體。非暫時性資料載體包含揮發性及非揮發性記憶體，諸如磁性、光學或固態類型之永久及非永久儲存媒體。仍在「資料載體」之範疇內，此等記憶體可為固定安裝或便攜的。

【0014】 在本發明中，「檔案」在廣義上用於指代一檔案系統中之任何獨立可儲存及/或可處理之資料集，包含一資料庫、檔案存檔或其他資料儲存內容脈絡。為了避免回應於一消除請求之不必要資料移除，一資料接收者通常將希望以儘可能小之塊(即，通常以一每檔案方式)處置含有個人資料之媒體。本發明符合此願望，此係因為其不僅容許檔案，而且容許一檔案之子集在一人之個人資料已被消除之後被救回。重溫上文列出之實例，一檔案可例如對應於一影像、一視訊序列、一資料庫或一文件。

【0015】 本發明努力使用術語「個人資料」、「資料主體」(即，一自然人)、「資料接收者」(即，至少向其揭示個人資料之一方)及「假名化」以與其等在GDPR中之含義一致。因此，一「個人資料項目」係「個人資料」之一項目，諸如含有一人之臉之一影像之一區域、其中可見一私人擁有之汽車之牌照之一視訊圖框、含有一人之姓名之一資料庫列或含有一人之認證之一文件之一區段。

【0016】 一般言之，發明申請專利範圍中使用之全部術語應根據其等在技術領域中之普通含義來解釋，除非本文中另外明確定義。對「一/一個/該元件、設備、組件、構件、步驟等」之全部參考應被開放性地解釋為指代元件、設備、組件、構件、步驟等之至少一個例項，除非另外明確規定。本文中揭示之任何方法之步驟不必以所揭示之確切順序執行，除非明確規定。

【圖式簡單說明】

【0017】 現參考隨附圖式藉由實例描述態樣及實施例，其上：

圖1係用於儲存含有個人資料之一檔案之一方法之一流程圖；

圖2係用於消除與一人相關聯之個人資料之一方法之一流程圖；

圖3係用於將個人資料恢復至一所儲存檔案中之一方法之一流程圖；

圖4係用於至少執行圖1中繪示之方法之一裝置之一功能方塊圖；及

圖5展示一金鑰導出結構，其中各箭頭表示一單向映射。

【實施方式】

【0018】 現將參考隨附圖式在下文中更充分描述本發明之態樣，其上展示本發明之特定實施例。然而，此等態樣可以許多不同形式體現且不應被解釋為限制性；實情係，藉由實例提供此等實施例，使得本發明將為透徹且完整的，且將本發明之全部態樣之範疇充分傳達給熟習此項技術者。在描述各處，相同數字指代相同元件。

儲存含有個人資料之一檔案

【0019】 圖1繪示用於儲存含有個人資料之一檔案之一方法100。方法100可由已接收或產生檔案且已進一步獲得一人同意將其個人資料儲存在檔案中之一資料接收者、一自然人或法人執行或代表其等執行。該同意不僅可涵蓋待儲存之檔案中之個人資料，而且涵蓋額外檔案。方法100已經設想以處置其中該人撤銷其同意之場景；撤銷可等效於完全消除該人之個人資料之一請求。

【0020】 在一初始選用步驟110中，使用一預定義單向函數組態之一單向函數介面(參閱圖4，元件490)可用於一人以容許其基於一私密識別符(PrivID)及待儲存之檔案之一符記(FileID.m)之一組合來產生一臨時匿名識別符(AnonID.m)。單向函數介面可用作本端安裝之軟體或一線上介面，其經鋪設，使得該人可在不與資料接收者共用私密識別符(PrivID)的情況下產生臨時匿名識別符(AnonID.m)。僅當該人希望消除其個人資料時，私密識別符(PrivID)之共用可為必要的，如下文參考圖2說明。

【0021】 作為單向函數，方法100之實施方案可使用一雜湊函數，特定言之，提供考慮到待儲存之個人資料之敏感性而被視為足夠之一安全等級之一密碼雜湊函數。兩個實例係SHA-256及SHA3-512。單向函數應為預定義的(例如，其應為可再現的)，使得當待執行一消除請求時，可再生臨時匿名識別符(AnonID.m)。

【0022】 在步驟110中可用於該人之單向函數介面可進一步容許該人基於一個人識別符(ID)產生私密識別符(PrivID)。個人識別符(ID)可為一民用或官方識別符，諸如一識別號碼、社會安全號碼、護照號碼、姓名及出生日期之組合等，該人可在無需主動存檔的情況下重建該識別符。如果此優點不被視為重要的，則該人可向單向函數介面提供一任意位元模式作為私密識別符(PrivID)，只要該人確信其可再現與一未來消除請求有關之位元模式，且位元模式對於第三方而言相當難以再現。從個人識別符(ID)至私密識別符(PrivID)之映射可為與用於將私密識別符(PrivID)映射至臨時匿名識別符(AnonID.m)相同之單向函數；替代地，可使用一不同單向函數。無論哪種方式，除非該人已可靠地儲存私密識別符(PrivID)，否則其應確保其可存取相同單向函數或將來亦可存取單向函數，以仍能夠命令消除其個人資料。

【0023】 待儲存之檔案之符記(FileID.m)係任意的，只要其可基於關於儲存在第二記憶體中之檔案之資訊來重建。符記(FileID.m)可為一執行序號。為了容許追溯枚舉(例如，當已請求消除時)，符記較佳地係一離散量。實例符記包含檔案建立日期、媒體記錄資料、檔案(檔案之匿名化版本之)大小、一預定義大小格集中之檔案大小所屬之一大小格(例如，在範圍[0,10]、[10,20]、[20,30]、...內之MB大小)、檔案內容之一指紋/摘

要、識別檔案系統中之檔案之一檔案名稱等。為了實行個人資料消除，資料接收者可藉由查詢關於儲存在第二記憶體中之全部檔案之一檔案系統來追溯地獲得此等符記之完整值集。如果檔案建立日期被用作符記，則一完整值集對應於檔案儲存已進行之資料範圍，例如，其可從一工作日誌以一數位或非數位格式讀取。雖然對本發明並非必要，但針對各檔案使用一唯一符記(即，一識別符)具有一些優點，因為此確保在項目特定匿名識別符(AnonID.m.n)之間不存在衝突；替代地，相同符記(FileID.m)可用於在相同或鄰近時間點儲存之多個檔案之一叢集，使得無需儲存敏感臨時匿名識別符(AnonID.m)。然而，針對全部檔案使用一恆定符記並非明智的，因為此將暗示全部項目特定匿名識別符將屬於一共同序列，且使得無法高效地簿記所儲存之個人資料項目之總數；當請求完全消除時，此簿記非常方便。

【0024】 如果待儲存之檔案之符記(FileID.m)不為該人所知(例如，與今天之日期不同)，則在一第二選用步驟112中，其值可與該人共用，或可直接供應至單向函數介面。接著，可基於私密識別符(PrivID)及符記(FileID.m)之組合正確地產生臨時匿名識別符(AnonID.m)。方法100可包含步驟110或步驟112、此兩個步驟之組合或兩者皆不包含。

【0025】 在方法100之一下一步驟114中，獲得該人之一臨時匿名識別符(AnonID.m)。臨時匿名識別符(AnonID.m)隨檔案之符記(FileID.m)而變化。獲得臨時匿名識別符(AnonID.m)之一較佳方式係從該人接收其；以此方式，該人無需與執行方法100之資料接收者共用私密或個人識別符。

【0026】 在一步驟116中，提取與該人相關聯之個人資料項目。

【0027】 在一步驟118中，針對已在步驟116中提取之各個人資料項目，產生該人的一定位符(Loc.m.n)及一項目特定匿名識別符(AnonID.m.n)。

【0028】 定位符(Loc.m.n)容許將個人資料項目恢復至檔案中。其結構可取決於與檔案有關之媒體類型。如果個人資料項目係一影像之一區域，則定位符(Loc.m.n)可例如鑑於其定界框座標來指示影像中之該區域。針對視訊資料，容許在一圖框中恢復對應於該人之臉或其汽車牌照之一提取區域的一定位符可指示圖框之一序號及提取區域之影像座標。

【0029】 在步驟118中，藉由將一預定義單向函數應用於臨時匿名識別符(AnonID.m)及個人資料項目之一識別符(n)之一組合來產生該人之項目特定匿名識別符(AnonID.m.n)。單向函數可相同於由該人用於產生臨時匿名識別符(AnonID.m)之函數，或其可為具有類似特性之一不同單向函數。個人資料項目之識別符(n)可為一檔案特定序號，即，針對待儲存之各新檔案或(視情況而定)針對待同時儲存之各檔案叢集重設序列計數器，使得各識別符在其檔案(檔案叢集)內係唯一的，但屬於兩個不同檔案(檔案叢集)之個人資料項目可具有相同識別符。識別符(n)可進一步為一全域序號，或其可為在作業系統或另一相關命名空間之位準上之個人資料項目之一完整識別符。代替一數字計數器，吾人可等效地使用一字母計數器或在任何適合離散集或空間中取值之一計數器。計數器可使用一預定義枚舉(或遞增)規則 $n_{k+1} = f(n_k)$。

【0030】 在方法100之一進一步發展中，其中可儲存一檔案之連續版本，當待儲存新版本時，重複步驟118，藉此個人資料項目之定位符(Loc.m.n.v)進一步取決於檔案之一版本(或提交) v。此支援在第二記憶體

中實施版本控制。

【0031】參考圖5，其繪示識別符ID、PrivID、AnonID.m、AnonID.m.n如何相關。各向下箭頭對應於一單向函數之應用。圖5之左手側上之字母進一步指示哪個實體存取所關注識別符。

A：私密識別符(ID)與資料主體保持在一起；從來無需與資料接收者共用。

B：資料主體儲存私密識別符(PrivID)，直至儲存個人資料之同意被撤銷。此時，資料主體與資料接收者共用私密識別符(PrivID)以容許資料接收者根據方法200消除其個人資料。

C：資料主體與資料接收者共用臨時匿名識別符(AnonID.m)之一者等效於同意儲存具有其個人資料之檔案。資料接收者使用此識別符以根據方法100實行檔案之儲存。

D：資料接收者將項目特定匿名識別符(AnonID.m.n)與所提取個人資料項目一起儲存在第一記憶體中。為了容許資料接收者根據方法200實行對個人資料項目之一所請求消除，此等識別符無法被刪除，直至個人資料項目被刪除。

【0032】返回至圖1，方法100進一步包括一步驟120，其中將各個人資料項目與定位符(Loc.m.n或Loc.m.n.v)及項目特定匿名識別符(AnonID.m.n)一起儲存在第一記憶體中(參閱圖4，元件421)。一關聯式資料庫可用於此儲存操作，其可被可視化為具有以下一般外觀之一表：

表1：第一記憶體之實例資料結構		
定位符	個人資料項目	項目特定匿名識別符
Loc.1.1	人之臉之第一圖像	AnonID.1.1
Loc.1.2	人之臉之第二圖像	AnonID.1.2
…	…	…

【0033】 在一選用步驟122中，例如，將該人之一計數器條目儲存在第一記憶體中或別處。計數器條目容許驗證與該人相關聯之全部個人資料項目之一枚舉之詳盡性。為此，計數器條目可指示：

- 個人資料項目之總數，在此情況中，消除方法應用一預先商定之枚舉規則及一開始規則，

- 第一及最後個人資料項目(例如，鑑於其等之項目特定匿名識別符AnonID.m.n，或鑑於其等之定位符Loc.m.n)，在此情況中，消除方法應用一枚舉規則，

- 全部個人資料項目之一清單，在此情況中，消除方法可為不可知的，或

- 全部個人資料項目之位置之一清單或其等之位置，在此情況中，消除方法可為不可知的。

較佳地，針對含有該人之個人資料之各檔案或針對所使用之各新檔案符記(FileID.m)儲存一個計數器條目。

【0034】 在一些實施例中，計數器條目包含該人之一可辨識匿名識別符(RecAnonID.m)，其藉由將單向函數應用於臨時匿名識別符(AnonID.m)而產生，如由圖5中之虛線箭頭指示。由於可辨識匿名識別符(RecAnonID.m)已藉由一單向函數產生，因此無法將其歸因於該人。然而，可辨識匿名識別符(RecAnonID.m)容許在實行一消除請求時驗證是否

已定位正確人之計數器條目。當計數器條目包含可辨識匿名識別符(RecAnonID.m)時，其可具有以下結構：

表2：計數器條目之實例資料結構	
可辨識匿名識別符	個人資料項目之總數
RecAnonID.1	N1
RecAnonID.2	N2
…	…

此可被理解為如下：已使用符記FileID.1之一或多個檔案含有與該人相關聯之確切N1個個人資料項目，已使用符記FileID.2之一或多個檔案含有與該人相關聯之確切N2個個人資料項目，且以此類推。

【0035】 在方法100之一進一步選用步驟124中，採取動作以防止臨時匿名識別符(AnonID.m)之非揮發性儲存。此等保護措施可包含消除一執行時記憶體中之識別符或對其進行覆寫；替代地，第一記憶體及第二記憶體以及任何可用進一步非揮發性記憶體具備拒絕儲存具有臨時匿名識別符(AnonID.m)之資料類型之資料之一閘管理器功能性。以此方式，如果將在第二天儲存一新檔案(假定此時段過長而無法在執行時記憶體中維持識別符)，則需要獲得一新臨時匿名識別符(AnonID.(m+1))，即，重新執行步驟114。

【0036】 此時，在步驟126中，評估待儲存之檔案是否含有與任何另一人相關聯之個人資料。如果情況如此(「是」分支)，則執行循環返回以針對該另一人實行步驟114、116、118及120 (以及選用步驟110及112，如果包含)。因此，獲得另一人之一臨時匿名識別符(AnonID'.m)；提取與另一人相關聯之個人資料項目；及針對各個人資料項目產生另一人的一定位符(Loc.m.n)及一項目特定匿名識別符(AnonID'.m.n)。應注意，

兩個人之定位符可取決於屬於相同序列之一識別符(n)。

【0037】 如果針對待儲存之檔案無需考慮其他人(來自步驟126之「否」分支)，則方法100之執行繼續至一選用步驟128，其中移除檔案中之個人資料項目以獲得檔案之一匿名化(或審查)版本。該移除可藉由移除(刪除)個人資料項目、廢除個人資料項目中之可能辨識因素、隱藏、編輯、遮罩、替換或覆寫個人資料項目或此外應用適合篩選或影像處理之至少一者來達成。適合篩選及影像處理包含賦予模糊、像素化、變形或傾向於使個人資料無法識別之其他效應之篩選及影像處理。此篩選或影像處理通常具有資料破壞類型，且將減少檔案之資訊內容。

【0038】 在一隨後步驟130中，將不具有個人資料項目之檔案之匿名化版本儲存在一第二記憶體中(參閱圖4，元件422)。第二記憶體可為與第一記憶體相同之記憶體。然而，在一些實施例中，第二記憶體不同於第一記憶體。

【0039】 在步驟130內，全部所提取個人資料項目之定位符(Loc.m.n)可視情況與檔案之匿名化版本一起儲存。換言之，此選項意謂定位符(Loc.m.n)儲存在第一記憶體及第二記憶體兩者中。在檔案最初含有之一些個人資料已被消除且已藉由刪除表1中與請求人相關聯之全部列(包含定位符)來執行此消除之一狀況中，當將重建檔案時，存取定位符(Loc.m.n)之一備用複本係有幫助的。接著，定位符之備用複本(Loc.m.n)容許將對應位置標記為空/修改/無效，儘管進行消除。替代地，如果消除操作保留定位符(即，其使表1之第一行保持不變)，則可實施相同標記功能性。

【0040】 此完成檔案之一第一版本之儲存。

【0041】 視情況，方法100可擴展至一第二檔案之儲存，該第二檔案亦含有與該人相關聯之個人資料。第二檔案可藉由屬於相同時間、空間或標的物內容脈絡而與第一檔案相關。例如，該等檔案可表示在連續時間點獲取之影像，或彼此接續之視訊序列。該等檔案可進一步關於一成像空間之不同子區域，該成像空間已被分區以獲得可管理檔案大小、粒度或類似物。

【0042】 因此，在一步驟132中評估是否將儲存一第二檔案，在此情況中(「是」分支)，執行循環返回，在步驟114開始。在此執行回合中，獲得該人之一第二臨時匿名識別符(AnonID.(m+1))，該臨時匿名識別符(AnonID.(m+1))取決於第二檔案之一符記(FileID.(m+1))。從第二檔案提取與該人相關聯之個人資料項目。針對各所提取之個人資料項目，產生該人的一定位符(Loc.(m+1).n)及一項目特定匿名識別符(AnonID.(m+1).n)。將各個人資料項目與定位符及項目特定匿名識別符一起儲存在第一記憶體中。最後，將不具有個人資料項目之第二檔案之一匿名化版本儲存在第二記憶體中。

【0043】 如果不再儲存檔案(來自步驟132之「否」分支)，則方法100之執行可終止。

【0044】 在方法100之一選用額外步驟134中，將檔案之一經更新匿名化版本儲存在第二記憶體中。經更新匿名化版本可在版本控制下儲存，即，先前匿名化版本未從第二記憶體刪除。可在無需更新第一記憶體中之資訊(其保持有效)的情況下執行經更新匿名化版本之儲存；此事實有利地可限制受託處理個人資料之人員之範圍。

【0045】 視情況，步驟134影響第一記憶體及第二記憶體兩者中之

資料。假定期望增加一視訊序列中之亮度，則此影像處理操作可應用於視訊序列之全部圖框及第一記憶體中之全部裁剪影像(即，所提取之個人資料項目)。匿名化視訊序列作為一新版本保存在版本受控之第二記憶體中，且針對新版本(v=2)產生儲存在第一記憶體之資料結構中之新列上之新定位符(Loc.m.n.2)。各新列包含經修改(變亮)裁剪影像，但具有與第一版本相同之AnonID.m.n。此在不損害個人隱私之保護的情況下變得可能。

消除與一人相關聯之個人資料

【0046】 圖2以流程圖形式繪示用於從一第一記憶體消除與一人相關聯之個人資料之一方法200。方法200在記憶體儲存個人資料項目以及與個人資料項目相關聯之人之對應定位符(Loc.m.n)及項目特定匿名識別符(AnonID.m.n)之一時間點起始；作為執行上文描述之用於儲存含有個人資料之一檔案之方法100之一結果，此內容可已被載入至記憶體中。

【0047】 方法200可例如由已在先前接收或產生一或多個檔案且已獲得該人同意儲存其在檔案中含有之個人資料之一資料接收者、一自然人或法人執行或代表其等執行。用於消除與該人相關聯之個人資料之方法200可在該人請求「被遺忘」(使其個人資料被消除)時執行，或等效地，在該人撤銷先前給出之同意時執行。

【0048】 在方法200之一第一步驟210中，獲得該人之一私密識別符(PrivID)。由於資料接收者在用於儲存檔案之方法100之一正常執行實施方案期間未從該人接收任何私密識別符(PrivID) (此共用不會改良該人之隱私)，步驟210通常將需要從該人接收私密識別符(PrivID)或從該人授予資料接收者讀取存取之一共用記憶體檢索私密識別符(PrivID)。

【0049】 在一第二步驟212中，獲得可已從中提取個人資料項目之全部檔案之符記(FileID.m)。在此步驟212中，資料接收者可根據與含有個人資料之一或多個檔案之儲存有關之一規則及/或文件再生符記(FileID.m)。替代地，從一記憶體接收或提取符記(FileID.m)。

【0050】 原則上，該人可維持其本身註冊之符記(FileID.m)，且與資料接收者共用與刪除請求有關之符記；此將容許該人將其請求限制為一部分消除，例如消除在一特定日期記錄之檔案中含有之個人資料。然而，如果資料接收者係一專業實體，則一更方便選項可為資料接收者儲存足夠資訊以容許其自身詳盡地再生符記(FileID.m)，而無需來自該人之除私密識別符(PrivID)之外之任何其他輸入。此資訊之儲存應至少與私密資料之儲存一樣可靠及/或持久，因為如果資訊丟失，則不再存在任何方便方式來基於與一特定人有關之私密資料之知識執行選擇性刪除。如果符記(FileID.m)係基於檔案名稱、原始檔案大小、建立日期或其他檔案屬性，則可實踐之一有吸引力之選項係資料接收者查詢一第二記憶體，該第二記憶體儲存已從其中提取個人資料項目之檔案之匿名化版本。接著，在一子步驟212.1中，查詢可包含向第二記憶體之檔案系統發出之一ls或dir命令，只要第二記憶體儲存所關注檔案，該命令便將成功。由於在一隨後步驟224中，從查詢之輸出導出之符記將與所產生之項目特定匿名識別符(AnonID.m.n)匹配，因此如果對第二記憶體之查詢作為一副產品傳回與該人無關之額外檔案之屬性，則其係一非常小問題。

【0051】 在下一步驟214中，針對檔案符記(FileID.m)之各者，獲得與該人相關聯且可已從對應一或多個檔案提取的全部個人資料項目之識別符(n)。此等識別符(n)之獲得可包含從記一記憶體或其他實體檢索其等，

或可基於一再生程序。再生程序可由從該人接收之私密識別符(PrivID)控制，且可進一步取決於儲存在由資料接收者維持之一記憶體中之資訊。

【0052】 例如，可藉由執行一子步驟214.1來獲得待消除之個人資料項目之識別符(n)，其中讀取該人之一計數器條目。上文結合用於儲存之方法100之步驟122介紹一計數器條目之概念，以及視情況包含一可辨識匿名識別符(RecAnonID.m)之一實例資料結構。為了在多個所儲存計數器條目中找到一檔案之正確計數器條目，資料接收者藉由首先將單向函數應用於私密識別符(PrivID)及檔案之符記(FileID.m)之組合(其傳回一臨時匿名識別符(AnonID.m))且接著將單向函數應用於臨時匿名識別符(AnonID.m)而再生可辨識匿名識別符(RecAnonID.m)。資料接收者將此操作之輸出與多個所儲存計數器條目之相關欄位(行)匹配。匹配計數器條目之另一欄位將表示個人資料項目之總數、由一預定義枚舉規則判定之一序列中之第一及最後個人資料項目、全部個人資料項目之一清單或在步驟122下列出之任何其他選項。因此，由於各臨時匿名識別符(AnonID.m)預期一個計數器條目，因此子步驟214.1針對各臨時匿名識別符(AnonID.m)傳回一組識別符(n)。

【0053】 為了繪示，假定計數器條目指示所儲存之第一個人資料項目之一識別符(n_a)及最後個人資料項目之一識別符(n_b)。此處，「第一」及「最後」指代識別符之枚舉序列，而不一定係儲存個人資料項目之時間點。在此情況中，消除方法200應用一枚舉規則$n_{k+1} = f(n_k)$，其相同或等效於儲存方法100中使用之一對應枚舉規則。藉由將枚舉規則應用於第一個人資料項目之識別符(n_a)，且接著遞迴至連續輸出，直至已到達最後個人資料項目之識別符(n_b)，資料接收者可再生全部識別符。儲存在計數器

條目中之最後個人資料項目之識別符(n_b)用於驗證所枚舉識別符之詳盡性。在此再生程序之變體中，可預先商定或預先指定第一個人資料項目之識別符(n_a)。此外替代地，指示識別符之總數之一計數器條目將與知道所儲存之最後個人資料項目之識別符(n_b)一樣有用。

【0054】 在一進一步步驟216中，藉由將一預定義單向函數應用於所獲得私密識別符(PrivID)及所獲得檔案符記(FileID.m)之組合來產生該人之臨時匿名識別符(AnonID.m)。單向函數在其動作等效於當儲存含有個人資料之一或多個檔案時用於產生臨時匿名識別符(AnonID.m)之單向函數之意義上係預定義的。

【0055】 如熟習此項技術者將瞭解，步驟214及216可依任何順序執行，或並行執行。由於在步驟216中產生之臨時匿名識別符(AnonID.m)可用作子步驟214.1中之一輸入，因此並行執行可減少必須評估單向函數之總次數。

【0056】 此後接著產生該人之項目特定匿名識別符(AnonID.m.n)之一步驟218，其藉由針對該人之各所產生臨時匿名識別符(AnonID.m)將預定義單向函數應用於臨時匿名識別符(AnonID.m)及個人資料項目之所獲得識別符(n)之組合來進行。為了確保完全消除，步驟218應產生已用於儲存與該人相關聯之個人資料項目之該等項目特定匿名識別符(AnonID.m.n)之一完整集合。如果已使用子步驟214.1獲得識別符(n)，則各臨時匿名識別符(AnonID.m)存在一組識別符(n)；接著，組合此等集合之一者中之識別符(n)與對應臨時匿名識別符(AnonID.m)應為足夠的，而與一不同臨時匿名識別符(AnonID.m')組合不太可能提供匹配所儲存個人資料項目之任何者之進一步項目特定匿名識別符。

【0057】 在步驟220中評估該人之任何其他所產生臨時匿名識別符(AnonID.m)是否仍在步驟218中處理。如果否(「否」分支)，則在步驟222評估是否存在已用於儲存與該人相關聯之個人資料項目之任何進一步檔案符記(FileID.m)。如果發現存在此等進一步檔案符記(FileID.m)(「是」分支)，則針對各進一步檔案符記(FileID.m)重新向前執行步驟214。

【0058】 當已處理全部檔案符記(FileID.m)時，方法200繼續進行至步驟224，其中從第一記憶體消除匹配該人之所產生項目特定匿名識別符(AnonID.m.n)之任何者之全部此等個人資料項目。消除可僅針對個人資料項目，或可聯合刪除對應定位符及/或項目特定匿名識別符。後一選項對應於刪除由上文表1繪示之資料結構之完整列。如果期望定位已從中提取個人資料項目之檔案之部分(例如，出於標記目的)，則定位符應保持不變或以某一其他方式恢復，除非定位符之一複本已被儲存在別處。

將個人資料恢復至一所儲存檔案中

【0059】 圖3係用於將個人資料恢復至一檔案中之一方法300之一流程圖。方法300在一第一記憶體儲存個人資料項目以及與個人資料項目相關聯之人之對應定位符(Loc.m.n)及項目特定匿名識別符(AnonID.m.n)時及在一第二記憶體儲存檔案之一匿名化版本時之一時間點起始。作為執行上文描述之用於儲存含有個人資料之一檔案之方法100之一結果，記憶體可已接收此內容。此外，自儲存檔案之時間起，可已執行用於消除與一人相關聯之個人資料之方法200，在此情況中，第一記憶體現含有在執行儲存方法100時從檔案提取的個人資料項目之一不完整集合。

【0060】 在方法300之一第一步驟310中，從第一記憶體檢索已從該

檔案提取的該等個人資料項目及對應定位符(Loc.m.n)。如果定位符(Loc.m.n)亦已被儲存在除第一記憶體以外之一位置中，諸如第二記憶體，則其等可等效地從該處檢索。

【0061】 在一第二步驟312中，從第二記憶體檢索不具有個人資料項目之檔案之匿名化版本。

【0062】 在步驟314中，接著根據對應定位符(Loc.m.n)將個人資料項目恢復至檔案之匿名化版本中。例如，對應於一人之臉之一視訊圖框之一裁剪區域可被黏貼回至視訊圖框中，如定位符(Loc.m.n)中指示，此將視訊圖框恢復至類似於其原始狀態之一外觀。如果已儲存檔案之較新版本(例如，作為影像處理或視訊編輯之一結果)，則所恢復之視訊圖框可不同於原始條件。步驟314可需要檔案之一完全恢復，即，藉由恢復全部個人資料項目而不管其等與什麼人相關聯。

【0063】 子步驟314.1表示執行步驟314之一有利方式。此處，循序遍歷全部所檢索個人資料項目，且步驟314在最後項目之後終止。子步驟314.1將穩健地執行，即使當一些或全部個人資料已從第一記憶體消除時，例如，根據相關聯人之請求，且其可經組態以傳回具有對應於經消除個人資料項目之一些剩餘部分之一可用(未損壞、可讀、可編輯等)檔案。剩餘部分可含有在執行儲存方法100時應用之移除、隱藏、編輯、遮罩、替換、覆寫、篩選及影像處理之任何者之輸出。

【0064】 在一選用步驟316中，識別已提取但未恢復一個人資料項目之匿名化版本之此等部分。

【0065】 在一進一步選用步驟318中，向一下游效用處理步驟通知在步驟316中識別之部分。所識別部分可被理解為無效或人為修改之資

料，而非自然或代表性資料。例如，如果下游處理包含訓練一機器學習(ML)模型，則可從饋送至ML模型之訓練資料排除所識別部分。替代地，ML模型從所識別部分導出之任何更新(例如，如由一組更新權重、或計算梯度、或一神經網路之導出誤差表示)被刪除、中和或回滾至一先前值。

【0066】 具有恢復個人資料項目之檔案被保存在執行方法300之一處理器之一執行時記憶體中。為了加強資料主體之私密性，方法300可視情況包含採取動作以防止具有恢復個人資料項目之檔案之非揮發性儲存之一最終步驟320。此動作可包含在一執行時記憶體中消除檔案或在處理之後對其進行覆寫。替代地，第一記憶體及第二記憶體以及任何可用進一步非揮發性記憶體具備防止儲存檔案之一閘管理器功能性。此外替代地，可執行基於相依性追蹤技術之一清除。

裝置實施方案

【0067】 圖4展示一裝置410，其通信地連接至第一記憶體421及第二記憶體422，且包括經配置以執行儲存方法100、消除方法200及/或恢復方法300之處理電路411。處理電路411可含有特定應用或可程式化電路，或其等可使用網路連結(「雲端」)資源以一分佈方式實施。處理電路411可包含一揮發性執行時記憶體。替代地，記憶體可為非揮發性的，且具備一閘管理器或由相依性追蹤覆蓋。第一記憶體421可用於儲存從一檔案提取的經提取個人資料項目、定位符及項目特定匿名識別符。由於第一記憶體421用於相對敏感之內容，因此其應較佳地具有對入侵攻擊之一較高抵抗力。類似地，例如透過一網路至第一記憶體421之通信連接應受到保護以防止竊聽。第二記憶體422可用於儲存檔案之一匿名化版本(或多個匿名化版本)。記憶體421、422兩者皆可為非揮發性記憶體。第二記憶體422

可經受版本控制。第一記憶體421無需具有版本控制。

【0068】 圖4已用繪示如何執行儲存方法100之資料標籤進行註釋。在裝置410之左上側供應待儲存之一檔案。在左下側，供應一臨時匿名識別符(AnonID.m)。臨時匿名識別符(AnonID.m)可已使用一單向函數介面490由與私密資料相關聯之人產生或代表其產生。如指示，單向函數介面490接收該人之一私密識別符(PrivID)作為輸入，且根據裝置410供應之一檔案符記(FileID.m)進一步修改。該人可使用單向函數介面490 (在圖4中繪示為其之一進一步例項)以基於一個人識別符(ID)產生私密識別符(PrivID)。基於此等輸入，裝置410從所供應檔案提取個人資料項目(在圖4中符號化為一矩形及一圓形)，且將此等與定位符(Loc.m.n)及項目特定匿名識別符(AnonID.m.n)一起儲存在第一記憶體421中。接著，第一記憶體可含有個人資料項目、定位符及識別符之三組。與此並行，裝置410將檔案之一匿名化版本儲存在第二記憶體422中。

【0069】 當裝置410執行消除方法200時，其可接收請求人之一私密識別符(PrivID)，且其向第一記憶體421發出刪除命令。當裝置410執行恢復方法300時，其從第一記憶體421及第二記憶體422檢索資料，且輸出恢復檔案。

經編號實施例

實施例1.一種用於儲存含有個人資料之一檔案之方法(100)，該方法包括：

獲得(114)一人之一臨時匿名識別符(AnonID.m)，該臨時匿名識別符(AnonID.m)取決於該檔案之一符記(FileID.m)；

從該檔案提取(116)與該人相關聯之個人資料項目；

針對各個人資料項目，產生(118)容許將該個人資料項目恢復至該檔案中的一定位符(Loc.m.n)及該人之一項目特定匿名識別符(AnonID.m.n)，其中藉由將一預定義單向函數應用於該臨時匿名識別符(AnonID.m)及該個人資料項目之一識別符(n)之一組合來產生該項目特定匿名識別符；

將各個人資料項目與該定位符及該項目特定匿名識別符一起儲存(120)在一第一記憶體中；及

將不具有該等個人資料項目之該檔案之一匿名化版本儲存(130)在一第二記憶體中。

實施例2.如實施例1之方法，其用於進一步儲存含有與該人相關聯之個人資料之一第二檔案，該方法包括：

獲得(114)該人之一第二臨時匿名識別符(AnonID.(m+1))，該臨時匿名識別符(AnonID.(m+1))取決於該第二檔案之一符記(FileID.(m+1))；

從該第二檔案提取(116)與該人相關聯之個人資料項目；

針對各個人資料項目，產生(118)該人的一定位符(Loc.(m+1).n)及一項目特定匿名識別符(AnonID.(m+1).n)，其中藉由將該單向函數應用於該第二臨時匿名識別符(AnonID.(m+1))及該個人資料項目之一識別符(n)之一組合來產生該項目特定匿名識別符；

將各個人資料項目與該定位符及該項目特定匿名識別符一起儲存(120)在該第一記憶體中；及

將不具有該等個人資料項目之該第二檔案之一匿名化版本儲存(130)在該第二記憶體中。

實施例3.如實施例1或2之方法，其進一步包括：

獲得(114)另一人之一臨時匿名識別符(AnonID'.m)，該臨時匿名識別符(AnonID'.m)取決於該檔案之該符記(FileID.m)；

從該檔案提取(116)與該另一人相關聯之個人資料項目；

針對各個人資料項目，產生(118)該另一人的一定位符(Loc.m.n)及一項目特定匿名識別符(AnonID'.m.n)，其中藉由將該單向函數應用於該臨時匿名識別符(AnonID'.m)及該個人資料項目之一識別符(n)之一組合來產生該項目特定匿名識別符；及

將各個人資料項目與該定位符及該項目特定匿名識別符一起儲存(120)在該第一記憶體中，

其中該檔案之該匿名化版本經儲存在該第二記憶體中，而不具有與該人相關聯之該等個人資料項目及與該另一人相關聯之該等個人資料項目。

實施例4.如前述實施例中任一項之方法，其中該第二記憶體而非該第一記憶體經受版本控制。

實施例5.如前述實施例中任一項之方法，其中該第一記憶體及該第二記憶體係非揮發性的。

實施例6.如前述實施例中任一項之方法，其中：

該等個人資料項目之至少一者係一影像之一區域；且

該定位符(Loc.m.n)指示該影像中之該區域。

實施例7.一種用於將個人資料恢復至一檔案中之方法(300)，該方法包括：

從儲存已從檔案提取之個人資料項目以及與該等個人資料項目相關聯之人之對應定位符(Loc.m.n)及項目特定匿名識別符(AnonID.m.n)之一

第一記憶體檢索(310)已從該檔案提取的該等個人資料項目及對應定位符；

從一第二記憶體檢索(312)不具有該等個人資料項目之該檔案之一匿名化版本；及

根據該等對應定位符將該等個人資料項目恢復(314)至該匿名化版本中。

實施例8.如實施例7之方法，其中該恢復包含循序恢復(314.1)該等所檢索個人資料項目，且在最後項目之後終止。

實施例9.如實施例7或8之方法，其進一步包括：

識別(316)已提取但未恢復一個人資料項目之該匿名化版本之此等部分；及

向一下游效用處理步驟通知(318)該等所識別部分。

實施例10.如實施例7至9中任一項之方法，其進一步包括：

採取動作(320)以防止具有該等恢復個人資料項目之該檔案之非揮發性儲存。

【0070】 已在上文參考一些實施例主要描述本發明之態樣。然而，如由熟習此項技術者容易地瞭解，除上文揭示之實施例以外之其他實施例同樣可在本發明之範疇內，如由隨附專利發明申請專利範圍所定義。

【符號說明】

【0071】

100: 方法

110: 步驟

112: 步驟

114: 步驟

116: 步驟

118: 步驟

120: 步驟

122: 步驟

124: 步驟

126: 步驟

128: 步驟

130: 步驟

132: 步驟

134: 步驟

200: 方法

210: 步驟

212: 步驟

212.1: 子步驟

214: 步驟

214.1: 子步驟

216: 步驟

218: 步驟

220: 步驟

222: 步驟

224: 步驟

300: 方法

310: 步驟

312: 步驟

314: 步驟

314.1: 子步驟

316: 步驟

318: 步驟

320: 步驟

410: 裝置

411: 處理電路

421: 第一記憶體

422: 第二記憶體

490: 單向函數介面

【發明申請專利範圍】

【請求項1】

一種用於儲存含有個人資料之一檔案(file)之電腦實施方法，該電腦實施方法包括：

獲得一人之一臨時匿名識別符(temporary anonymous identifier)，該臨時匿名識別符取決於該檔案之一符記(token)；

從該檔案提取與該人相關聯之個人資料項目；

針對各個人資料項目，產生容許將該個人資料項目恢復至該檔案中的一定位符及該人之一項目特定匿名識別符，其中藉由將一預定義單向函數應用於該臨時匿名識別符及該個人資料項目之一識別符之一組合來產生該項目特定匿名識別符；

將各個人資料項目與該定位符及該項目特定匿名識別符一起儲存在一第一記憶體中；及

將不具有該等個人資料項目之該檔案之一匿名化版本儲存在一第二記憶體中。

【請求項2】

如請求項1之電腦實施方法，其進一步包括：

儲存該人之一計數器條目，該計數器條目容許驗證與該人相關聯之全部個人資料項目之一枚舉之詳盡性。

【請求項3】

如請求項2之電腦實施方法，其中該計數器條目包含藉由將該單向函數應用於該臨時匿名識別符而產生之該人之一可辨識匿名識別符。

【請求項4】

如請求項1至3中任一項之電腦實施方法，其由一資料接收者執行且進一步包括：

使經組態具有該預定義單向函數之一單向函數介面可用以容許一人基於一私密識別符及該檔案之該符記之一組合來產生該臨時匿名識別符，而無需與該資料接收者共用該私密識別符；及

視情況與該人或該單向函數介面共用該檔案之該符記。

【請求項5】

如請求項4之電腦實施方法，其中該單向函數介面經進一步組態以容許該人基於一個人識別符產生該私密識別符。

【請求項6】

如請求項1至3中任一項之電腦實施方法，其進一步包括：

採取動作以防止該臨時匿名識別符之非揮發性儲存。

【請求項7】

如請求項1至3中任一項之電腦實施方法，其進一步包括：

藉由包含移除、隱藏、編輯、遮罩、替換、覆寫、篩選、影像處理之至少一者之一匿名化操作移除該檔案中之該等個人資料項目以獲得該檔案之該匿名化版本。

【請求項8】

如請求項1至3中任一項之電腦實施方法，其進一步包括：

將該檔案之一經更新匿名化版本儲存在該第二記憶體中。

【請求項9】

如請求項1至3中任一項之電腦實施方法，其中：

該等個人資料項目之至少一者係一視訊序列中之一圖框之一區域；

且

該定位符指示該視訊序列中之該圖框且進一步指示該圖框中之該區域。

【請求項10】

一種用於從一第一記憶體消除與一人相關聯之個人資料之電腦實施方法，其中個人資料項目以及與該等個人資料項目相關聯之人之對應定位符及項目特定匿名識別符係由請求項1所指定的方式先前儲存，該方法包括：

獲得該人之一私密識別符；

獲得可已從中提取該等個人資料項目之全部檔案之符記；

針對該等檔案符記之各者，獲得與該人相關聯且可已從一對應檔案提取的全部個人資料項目之識別符；

藉由將一預定義單向函數應用於該所獲得私密識別符及該等所獲得檔案符記之組合來產生該人之臨時匿名識別符；

針對該人之各所產生臨時匿名識別符，藉由將該預定義單向函數應用於該臨時匿名識別符及該等個人資料項目之該等所獲得識別符之組合來產生該人之項目特定匿名識別符；及

從該第一記憶體消除匹配該人之該等所產生項目特定匿名識別符之任何者之全部個人資料項目。

【請求項11】

如請求項10之電腦實施方法，其中藉由查詢一第二記憶體來獲得可已從中提取該等個人資料項目之全部檔案之該等符記，其中已從中提取該等個人資料項目之該等檔案之匿名化版本係由請求項1所指定的方式先前

儲存。

【請求項12】

如請求項10或11之電腦實施方法，其中藉由檢索該人之一計數器條目來獲得全部個人資料項目之該等識別符。

【請求項13】

如請求項12之電腦實施方法，其進一步包括：

枚舉與該人相關聯之全部個人資料項目之識別符；及

基於該所檢索計數器條目驗證該等所枚舉識別符之詳盡性。

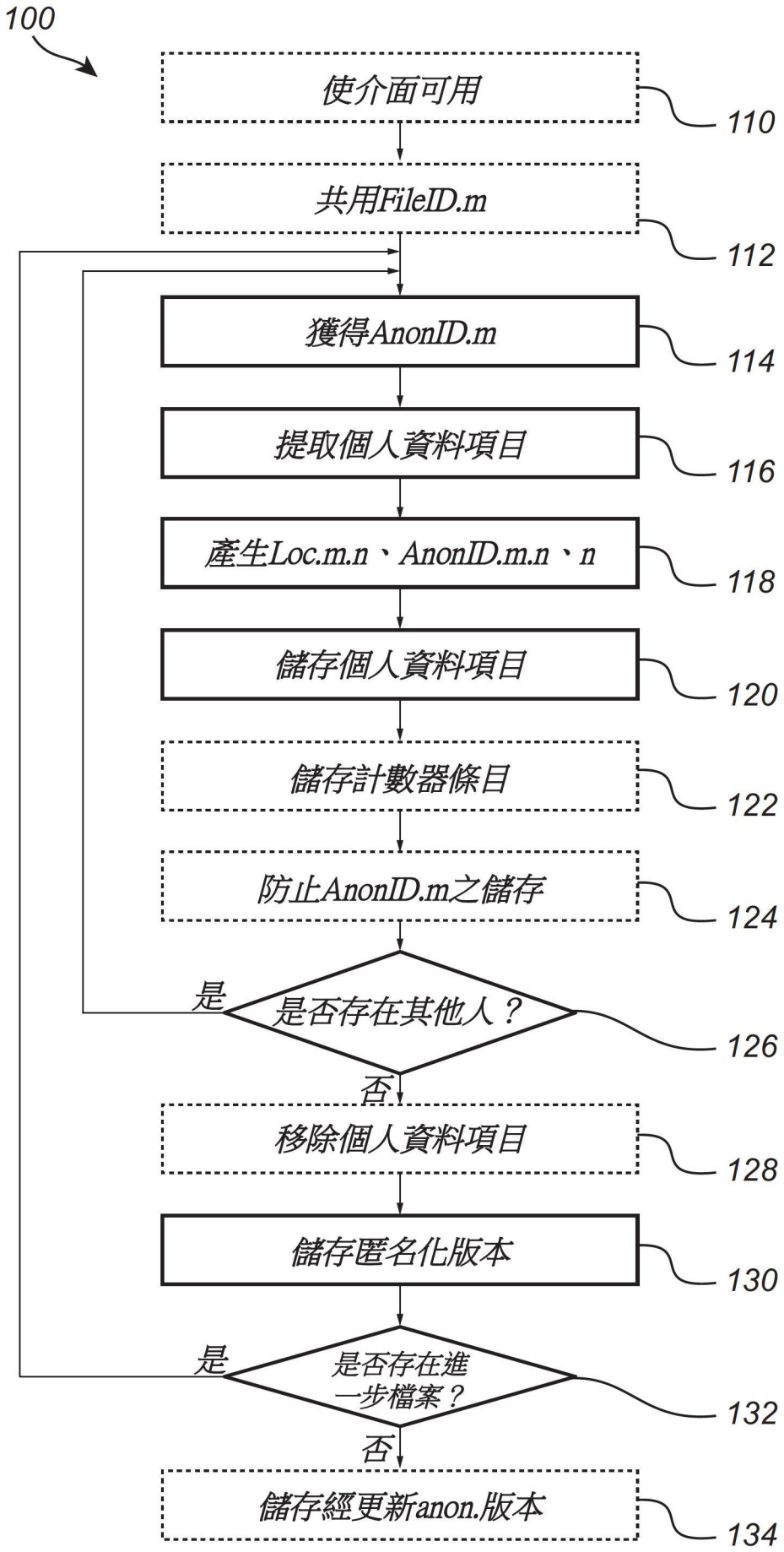
【請求項14】

一種儲存裝置，其可通信地連接至第一記憶體及第二記憶體且包括經配置以執行如請求項1至13中任一項之電腦實施方法之處理電路。

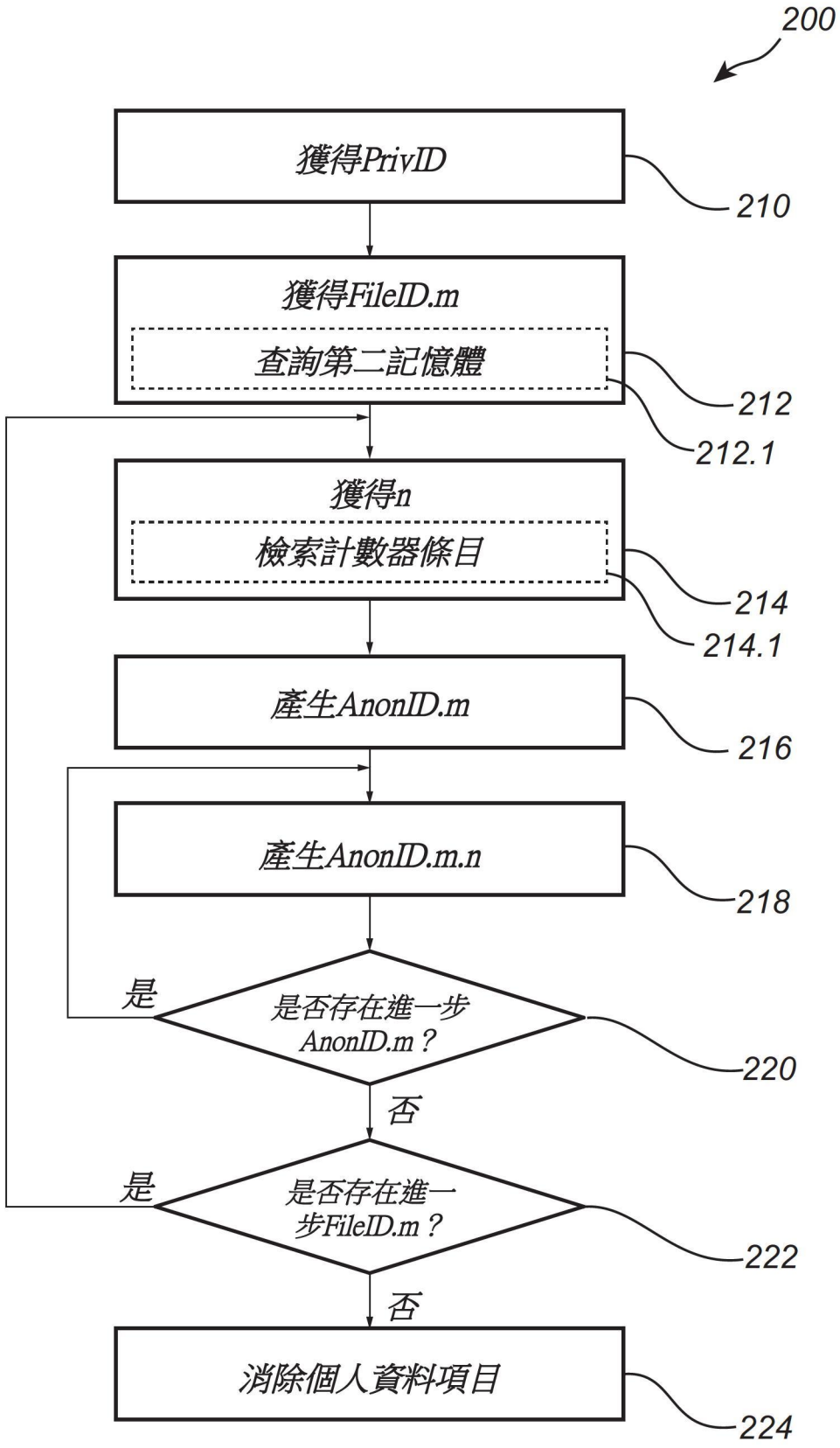
【請求項15】

一種電腦程式，其包括當其被一電腦所執行時，使該電腦實施如請求項1至13中任一項所述之電腦實施方法的指令。

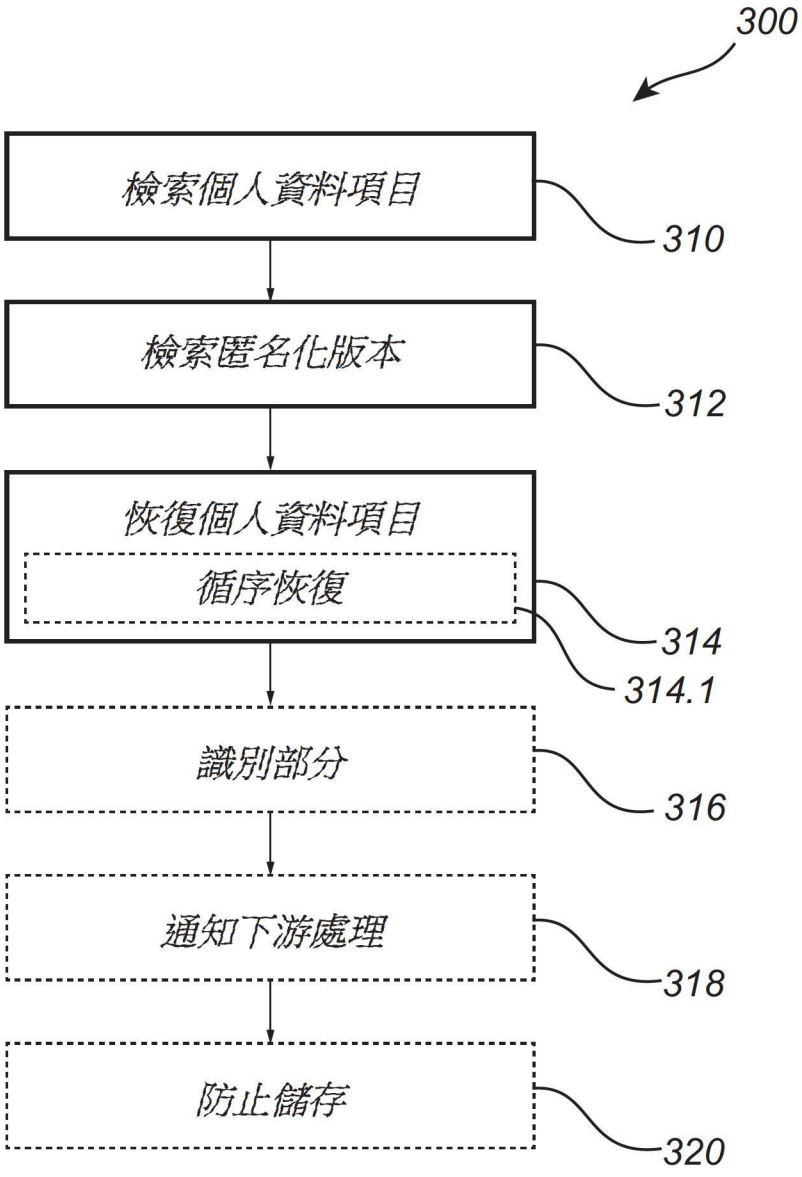
【發明圖式】


100
使介面可用
110
共用FileID.m
112
獲得AnonID.m
114
提取個人資料項目
116
產生Loc.m.n、AnonID.m.n、n
118
儲存個人資料項目
120
儲存計數器條目
122
防止AnonID.m之儲存
124
是
是否存在其他人？
126
否
移除個人資料項目
128
儲存匿名化版本
130
是
是否存在進一步檔案？
132
否
儲存經更新anon.版本
134

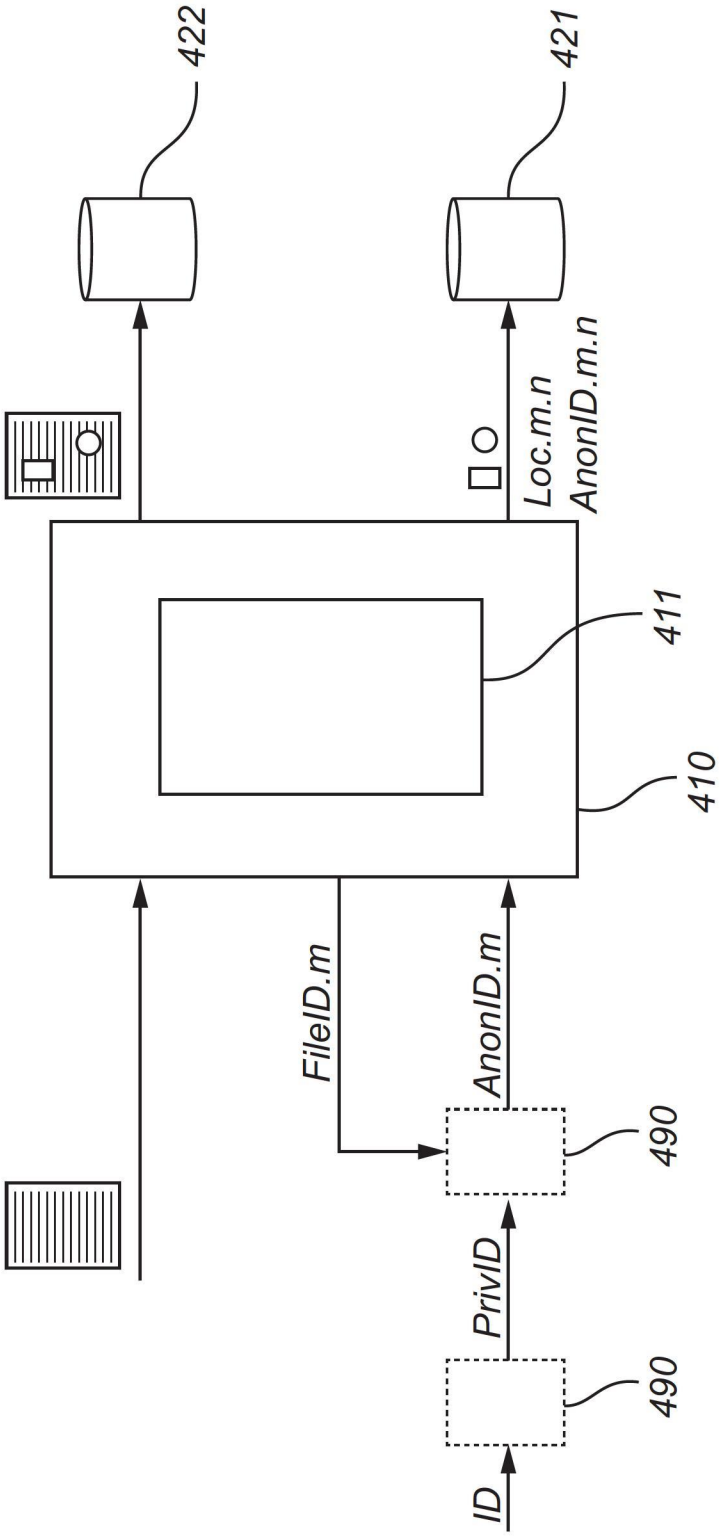
【圖1】


200
獲得PrivID
210
獲得FileID.m
查詢第二記憶體
212
212.1
獲得n
檢索計數器條目
214
214.1
產生AnonID.m
216
產生AnonID.m.n
218
是
是否存在進一步AnonID.m？
220
否
是
是否存在進一步FileID.m？
222
否
消除個人資料項目
224

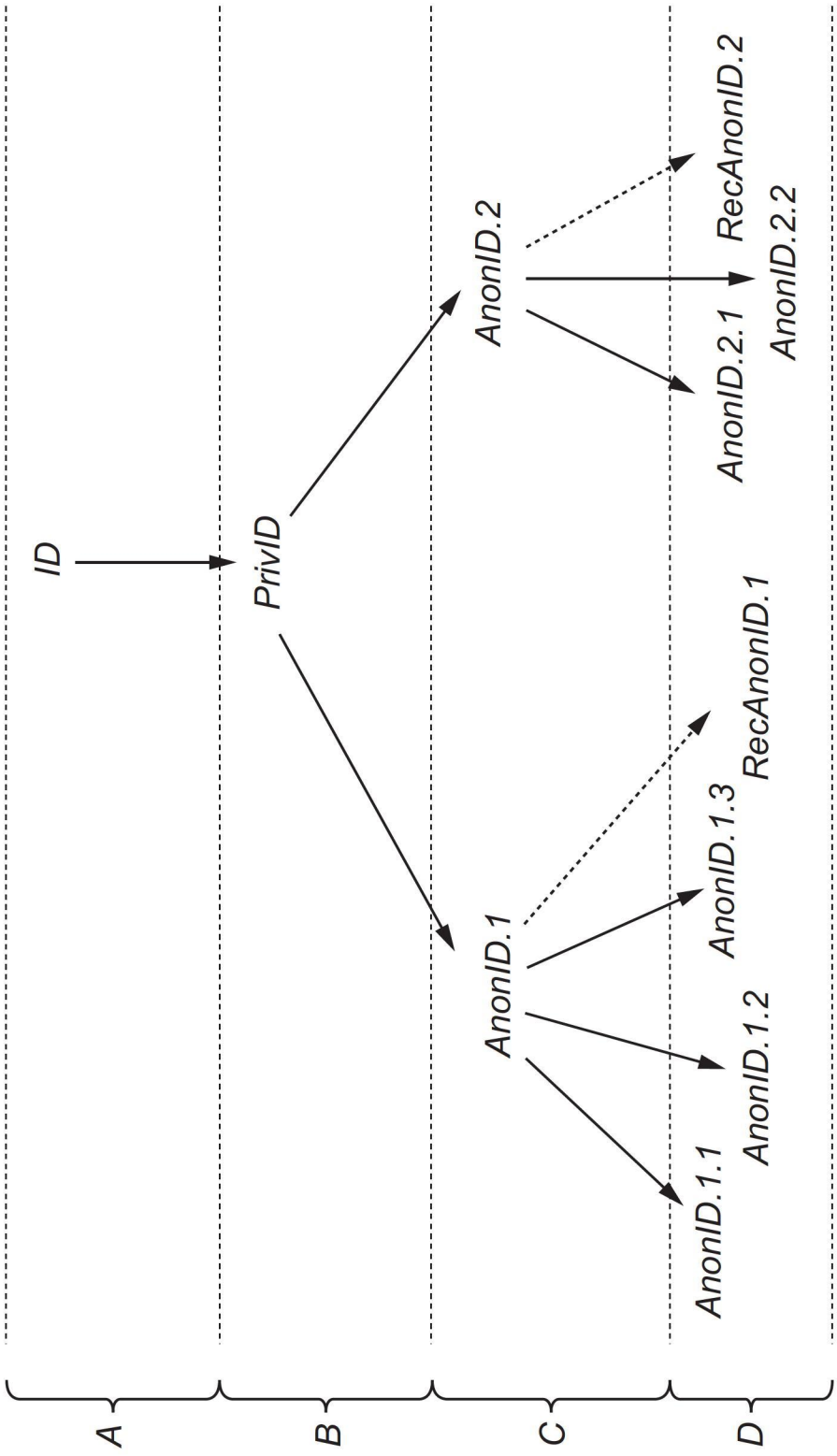
【圖2】


300
檢索個人資料項目
310
檢索匿名化版本
312
恢復個人資料項目
循序恢復
314
314.1
識別部分
316
通知下游處理
318
防止儲存
320

【圖3】


422
421
Loc.m.n
AnonID.m.n
411
410
FileID.m
AnonID.m
490
PrivID
490
ID

【圖4】


ID
PrivID
AnonID.2
AnonID.2.1
RecAnonID.2
AnonID.2.2
AnonID.1
AnonID.1.3
RecAnonID.1
AnonID.1.2
AnonID.1.1
A
B
C
D

【圖5】