106 年補助研究案

「通傳事業去識別化技術與相關技術規範研究」

補助研究報告

The Research on the Technical Specification of Personal Information De-Identification on Communication Industries

計畫主持人：蔡敦仁 博士
Project Coordinator：Dr. Tsai Dwe-Wren
計畫執行單位：財團法人電信技術中心
Executive Institution：Telecom Technology Center
計畫執行期程：106年3月1日至106年12月31日
Period of Project：March 1, 2017～December 31, 2017
計畫補助機關：國家通訊傳播委員會
Project DelegateInstitution：National Communications Commission
印製日期：中華民國 106 年 12 月 22 日
Date of Publication：December 22, 2017

「通傳事業去識別化技術與相關技術規範研究」

補助研究報告

執行單位

財團法人電信技術中心

計畫主持人

蔡敦仁

研究人員

蘇俊吉、許博堯、吳佩霏、林政諺

計畫編號：Y106-A9

GRB系統編號：PG10606-0090

執行期程： 106年3月1日至106年12月31日

補助機關：國家通訊傳播委員會

印製日期：中華民國106年12月22日

目　錄

圖　目　錄

表　目　錄

中文摘要

資通訊網路發展迅速，通訊傳播數據需求與日俱增，通訊傳播事業亟須去除個人資訊的有效程序與技術，個人資料去識別化可從紀錄或資料集中移除個人資訊，以保護個人隱私，在去識別化後，該資料集可認定為不包含個人資訊，依據個人資料保護法規定，如果資料集合無法辨識出特定個人，其資料處理與利用便不會侵犯個人隱私。個人資料去識別化雖無法排除重新識別的風險，但卻可以有效降低資料集合中識別特定個人的風險。

本計畫之目的在於參考國際間對於通訊傳播事業個人資料保護規範與去識別化機制進行分析，並提出去識別化技術規範草案，該規範將介紹個人資料去識別化的基本概念與程序，同時說明通訊傳播事業個人資料去識別化時要考量的關鍵措施，並提供通訊傳播事業在處理個人資料去識別化時遵循的指導原則。

關鍵詞：個人資料保護、隱私保護、通訊傳播、去識別化、重新識別

Abstract

As the demand for data communication increasing, institutions need effective processes and techniques to remove personal information. “De-identification” is the general term for removing personal information from a record or a data set. De-identification protects the privacy of individuals since a data set would be considered to be no longer contain personal information. If a person could not be identified through a data set, any data usage or utilizing would not be considered as the privacy violation of individuals. Although De-identification could not preclude the risk for Re-identify, it can effectively lower the risk for someone to be identified through a data set.

The purpose of this research is to refer and analyze other countries regulations on the Personal Data Protection Act and the “De-identification” issues. This research would present a technical specification draft for the De-identification that will introduce basic concepts and procedures as well as explaining the key steps for the de-identification in data communication. This research would provide a guideline for institutions to follow when they are going to remove personal information from data sets.

Keywords ： personal data protection, privacy, communication, de-identification, re-identification

第壹章　緒論

第一節 研究背景與動機

資通訊網路發展迅速，通訊與傳播產業間的藩籬已逐漸模糊，諸多網網相連形式的應用正掀起與人們生活息息相關的巨大變革，新型態的通訊傳播應用服務強調多元化、互動、客製化等特性。其中結合巨量資料分析方法，亦是發展創新經濟模式的趨勢，多樣性的巨量資料透過數據分析技術，使資料價值運用最大化。用戶使用新型態通訊傳播應用服務時，不免提供與用戶相關的個人資訊，包括身分、位置、消費、通訊、帳單明細、收視紀錄等相關資料，該類型資料或紀錄經過分析之後，對於通訊傳播服務業者無疑是具備商業價值的資訊。然而，對於此等具備商業價值資訊的運用，將涉及個人資料隱私議題，尤其是資料使用者容易在巨量資料中找到關聯性，得以直接或間接識別特定當事人，如何保護個人資訊已成為刻不容緩的課題。

在通訊傳播匯流趨勢下，國際個人資料與隱私保護相關組織已觀察到巨量資料與個人資料的安全疑慮，近年來開始頻繁進行研討與公告相關指引與標準。2014 年 5 月，國際電信個人資料保護工作小組(International Working Group on Data Protection in Telecommunications, IWGDPT）公布巨量資料與

隱私工作報告（Working Paper on Big Data and Privacy），說明巨量資料時代下可能面臨的隱私爭議發佈工作報告，其中將巨量資料價值鏈分為資料蒐集、彙整、分析、運用四階段。以通訊傳播事業而言，可能的個人資料蒐集來源包括：申辦通訊傳播服務之登記、手機應用、社群網站、帳單資訊、智慧電視、機上盒等，可能的個人資料運用方式包括：

- 分析瀏覽與收視紀錄，取得用戶偏好或關注事物；
- 分析位置資訊，瞭解用戶生活作息；
- 透過位置資訊鎖定用戶所在位置，投以廣告資訊；
- 串接以上個人資訊，產生數據分析結果，提供第三方，如廣告商、廣告主；
- 結合基本資料，強化用戶屬性剖繪（profile），進行精準廣告投遞。

通訊傳播業者如何運用個人資料取決於與用戶簽訂服務契約範圍，服務契約有關個人資料隱私部分則須符合資訊隱私權、自主權所涉及對個人資料運用的「事前知情」、「事中控制」及「事後退出」基本權利。

其次，我國政府於 103 年 10 月開始實行「個人資料保護法（其前身為電腦處理個人資料保護法）」，對於蒐集個人資料機關之蒐集、處理、利用個人資料等行為均有規範，且個人資料檔案保存應採取適當之安全措施，防範遭濫用、誤用等個人資料侵害情事，其中第 2 條第 1 款有關個人資料

之定義反面解釋可知，所謂去識別化，即指透過既定程序處理，使個人資料不再具有直接或間接識別性，亦即無從識別特定個人。同時經濟部標準檢驗局於 103 年至 104 年期間亦也公告確保 CNS 29100「資訊技術-安全技術-隱私權框架」國家標準，提供資通訊技術系統保護個人可識別資訊的高階框架，將組織、技術及程序各層面置於整體隱私權框架中，以及 CNS 29191「資訊技術－安全技術－部分匿名及部分去連結鑑別之要求事項」國家標準，期盼能達到政府機關開放資料「無從識別特定當事人」的成效，同時亦作為企業處理個人資料的參考指標。

去識別化係以整體個人隱私權保護為基礎，評估資料利用所伴隨的風險，須考量個人資料整體生命週期，包括隱私權政策、風險評估、去識別化操作、重新識別評鑑等程序。個人資料去識別化亦包括遮罩、重複抽樣、匿名等方法，視去識別化目的、資料欄位等因素，決定去識別化方法。為落實個人資料保護與隱私保護目的，本計畫旨在研究國際間通訊傳播事業用戶個人資料保護的管理規範，分析其中採用的通訊傳播事業個人資料去識別化機制，配合國內個人資料去識別化標準推展現況，積極與國家通訊傳播委員會及通訊傳播業者研討交流，進而制訂符合我國環境、可操作性之通訊傳播事業去識別化技術規範草案。

第二節 研究方法與目的

本計畫研究方法分述如下：

- 資料分析法：針對與研究主題相關案例，進行研究與比較分析。此方法將用以探討主要國家個人資料保護與去識別化相關規範，以作為我國在相關規劃上之借鏡。
- 深度訪談法：以去識別化之學者、專家及業者代表為對象，設計訪談議題，進行個別互動式、直接面對面或電話深入訪談，讓受訪者在訪談主題內闡述意見，以發掘受訪者信念、想法與態度。此方法將用於本計畫對產官學界意見之蒐集與分析。
- 焦點團體法：與個人資料去識別化相關之機關代表、學者、專家及業者代表為對象，舉辦公開說明會，適時提出本計畫之規劃方向，與各界進行雙向之意見交流。此方法將用於本計畫對產官學界意見之蒐集與分析。

本計畫冀望透過觀察國際間資通訊傳播政策與技術發展現況，發掘個人資料去識別化的相關議題，分析技術面向、政策面向、法規面向之因素，延伸至我國通訊傳播個人資料去識別化發展現況，俾利研擬符合消費者優先（pro-consumer）、投資優先（pro-investment）與競爭優先（pro-competition）之通訊傳播個人資料去識別化技術規範草案。

第三節 研究範圍與限制

一、 研究範圍

本計畫以「通訊傳播事業個人資料去識別化技術與相關技術規範研究」為主題，期望借鏡國際經驗及分析國內環境，為我國通訊傳播事業之個人資料去識別化技術與政策提出具體建議，並能兼顧資通訊事業發展及保護消費者權益。本計畫包含兩項分項工作（如圖 1），分項工作一「通訊傳播事業個人資料保護去識別化發展」進行國際通訊傳播事業個人資料保護與我國通訊傳播事業個人資料保護機制研究；分項工作二「我國通訊傳播事業個人資料去識別化技術規範草案」考量國內環境，包括國內法令規範與相關標準，以及業者做法，研擬適切之通訊傳播事業個人資料去識別化技術規範草案。

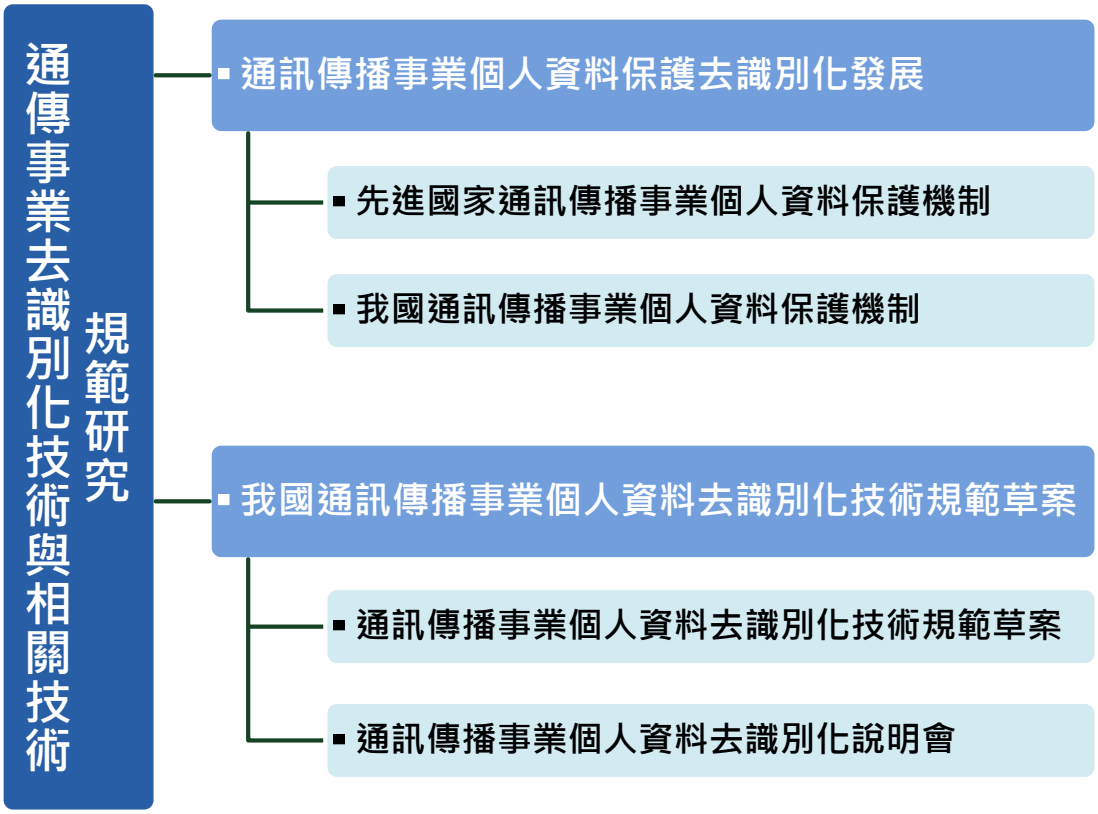

圖 1、本計畫架構圖

(一) 通訊傳播事業個人資料去識別化發展

近年來個人資料保護普遍受到國際間關注，國際間已有諸多國家制訂個人隱私保護法令與管理規範，同時基於個人資料隱私保護框架納入去識別化規範，亦有國際組織正致力於發展個人資料去識別化技術標準。個人資料保護首重個人隱私維護與保護責任，以確保個人隱私資料在蒐集、處理、利用過程中不受到侵害。

圖 2、個人資料保護

本分項工作針對先進國家與我國在個人資料保護去識別化機制進行研究，研究重點涵蓋個人資料保護法，以及通訊傳播事業個人資料與隱私保護相關的法令規範。

1. 先進國家通訊傳播事業個人資料保護機制

針對國際間主要國家之個人資料與隱私保護去識別化相關法令進行研究，就歐盟、美國、英國之基本法（個人資料保護法）、通訊傳播事業相關法令與指引，分析與通訊傳播事業蒐集、處理、利用個人資料有關去識別化之規範，例如：歐盟第 29 條資料保護工作小組「匿名化技術方法」意見書。

2. 我國通訊傳播事業個人資料保護機制

基於我國相關法令、管理條例與國家標準，研究目前適用國內通訊傳播事業之蒐集、處理、利用個人資料有關去識別化之規範，包含個人資料保護法，以及國家標準 CNS 29100 與 CNS 29191 推展現況，分析通訊傳播事業導入個人資料保護與去識別化之適法性。

(二) 我國通訊傳播事業個人資料去識別化技術規範草案

本分項工作旨在擬訂我國通訊傳播事業個人資料去識別化技術規範草案，首先請國家通訊傳播委員會協助函請通訊傳播業者回填個人資料去識別化自評表，召開說明會，向通訊傳播事業相關業者及專家學者說明本計畫緣由、目的與國內去識別化標準現況，同時配合業者訪談，瞭解業者個人資料隱私保護實務做法，以及對個人資料去識別化的看法與建議，進而擬訂通訊傳播事業個人資料去識別化技術規範草案。

1. 通訊傳播事業個人資料去識別化技術規範草案

(1) 物聯網— OTT 個人資料去識別化技術規範草案

OTT(Over-The-Top)以網際網路為基礎提供聲音、影音等媒體內容，毋須特定網際網路服務提供者（Internet Service Provider, ISP）或是特定有線電視多系統業者（Multiple-System Operator, MSO）的支持，OTT 業

者為獨立之網路內容業者。目前我國尚未對 OTT 服務監管發照，但國家通訊傳播委員會仍強調 OTT 業者需遵守「消費者保護法」、「個人資料保護法」等相關法令，OTT 業者蒐集的個人資料可能包括用戶基本資料、瀏覽內容、時段等。本計畫將制訂適合 OTT 服務之個人資料去識別化技術規範草案。

(2) 多媒體內容傳輸平台 MOD 個人資料去識別化技術規範草案

不同於 OTT，多媒體隨選系統（Multimedia on Demand, MOD）屬於 IPTV 商業模式，須綁定網際網路服務業者，甚至 IPTV 就是電信業者原生業務，國內則以中華電信 MOD 服務為主，MOD 服務蒐集的個人資料可能包括用戶基本資料、瀏覽內容、時段等，甚至在與用戶互動的雙向通訊時，用戶無意間透露更多的個人隱私。本計畫制訂適合 MOD 服務的去識別化技術規範草案。

(3) 有線電視個人資料去識別化技術規範草案

我國有線電視服務已非常普及，預計於今年（106 年）底國內有線電視系統台將全面數位化，透過數位機上盒（Digital Set Top Box），即可收視數位節目，數位機上盒區分單向與雙向通訊，雙向通訊具備資料回

傳的能力，始得用戶可以使用雙向互動的服務與功能，業者端則可能蒐集更多的個人隱私資訊。目前有線廣播電視系統工程查驗技術規範與有線廣播電視系統工程技術管理辦法尚未有個人資料隱私保護的相關要求，本計畫將制訂適合有線電視服務的個人資料去識別化技術規範草案。

2. 通訊傳播事業個人資料去識別化說明會

個人資料去識別化技術規範草案攸關通訊傳播事業對於個人資料處置管理，為確保技術規範草案之可操作，與通訊傳播相關業者交流討論為必要之務，引導業者瞭解個人資料隱私的重要性及可能面臨的資安威脅，藉由公開說明會做為通訊傳播業者、國家通訊傳播委員會與研究團隊之溝通交流平台，制訂適合我國通訊傳播事業環境、可施行於通訊傳播事業之技術規範草案。

二、 研究限制

受限於研究期程與經費，故研究方法以次級資料蒐集分析、說明會與專家訪談為主。且本計畫屬前瞻性標準研究，擬從政策、產業與技術三方面，研析通訊傳播事業去識別化相關議題，然現階段國際間普遍未規劃具體標準與規範，因此產業界通常不會特別關注該議題。雖如此，研究團隊將藉由說明會，以結構性的導引方式，對去識別化相關議題進行說明，力

求各界對於去識別化的觀點與精確性。

第四節 工作項目與期程

依本計畫補助契約與經核定之補助申請計畫書，本計畫之工作項目包含：通訊傳播個人資料保護去識別化發展，與我國通訊傳播事業個人資料去識別化技術規範草案，詳細工作項目如表 1。

一、 計畫進度表

表 1、計畫進度表

工作項目	工作月											
	1	2	3	4	5	6	7	8	9	10	11	12
分項 1：通訊傳播個人資料保護去識別化發展												
1.1 先進國家通訊傳播事業個人資料保護機制						▲						
1.2 我國通訊傳播事業個人資料保護機制						▲						
分項 2：我國通訊傳播事業個人資料去識別化技術規範草案												
2.1 通訊傳播事業個人資料去識別化技術規範草案												▲
2.2 通訊傳播事業個人資料去識別化說明會												
2.2.1 第一次說明會												▲
2.2.2 第二次說明會												▲
工作進度估計百分比 （%）			10	20	30	40	50	60	70	80	90	100

二、 計畫查核項目

表 2、計畫查核表

工作項目	查核時間		交付項目	
	期中	期末	報告	技術規範草案
分項 1：通訊傳播個人資料保護去識別化發展				
1.1 先進國家通訊傳播事業個人資料保護機制	●		●	
1.2 我國通訊傳播事業個人資料保護機制	●		●	
分項 2：我國通訊傳播事業個人資料去識別化技術規範草案				
2.1 通訊傳播事業個人資料去識別化技術規範草案		●		●
2.1.1 物聯網— OTT 個人資料去識別化技術規範草案		●		●
2.1.2 多媒體內容傳輸平台 MOD 個人資料去識別化技術規範草案		●		●
2.1.3 有線電視個人資料去識別化技術規範草案		●		●
2.2 通訊傳播事業個人資料去識別化說明會		●	●	
2.2.1 第一次說明會		●	●	
2.2.2 第二次說明會		●	●	

第貳章　通訊傳播個人資料保護去識別化發展

第一節 先進國家通訊傳播事業個人資料保護機制

一、 歐盟

(一) 個人資料保護規則[1]

1. 背景

1981 年，歐洲議會（European Parliament）通過個人資料保護協定，為歐洲國家制定個人資料保護法令之依據。1995 年，歐盟制定資料保護指令（EU Data Protection Directive），旨在改善歐洲各國之個人資料保護一致性、跨境傳輸個人資料與當事人同意，以及接收國保護措施的要求。只要是遵守個人資料保護指令的歐盟會員國，就等同採納各國的個人資料保護法，可以允許跨境資料傳輸。

由於歐盟資料保護指令在規範形式上為「指令（Directive）」，屬於歐盟地區廣泛共通的法律框架與指導原則，因此各會員國個人資料保護規範仍存在不一致之情形，不利於歐盟資料跨境傳輸目標，歐盟期盼能訂定具有

1 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN（last visited: May. 17, 2017）.

直接規範效力之「規則（Regulation）」[2]，歐盟執委會（European Council）遂於 2012 年開始資料保護規範修訂，2016 年 4 月歐洲議會通過歐盟規則 2016/679「個人資料保護規則（EU General Data Protection Regulation, GDPR）」，預期在 2018 年 5 月全面取代原資料保護指令。GDPR 法律位階屬於「規則」，將直接適用於歐盟各會員國，不需透過會員國國內法的轉換，且接受單一監理組織之監管（One stop shop）。此外，歐盟也將成立統一之「歐盟資料保護委員會（European Data Protection Board, EDPB）」，藉由發佈意見書（opinions）、指引（guidance）、建議等（recommendations）等，維持歐盟地區資料保護制度之跨國一致性。

2. 規範對象

規範對象區分「規範客體」以及「適用主體」。在規範客體方面，將規範範圍限定於「全部或部分以自動化方式蒐集、處理或利用的個人資料」，至於以「非」自動化方式蒐集、處理或利用的情形，但僅限於「建檔系統（filing system）」之部分（歐盟個人資料規則第 2 條第 1 項）。在「適用主體」方面，歐盟個人資料規則對於資料控制者（data controller）及處理者

[2] SeeFrancoise Gilbert, European Data Protection 2.0: New Compliance Requirements in Sight—What the Proposed EU Data Protection Regulation Means for U.S. Companies, 28 Santa Clara Computer &. High Tech. L. J. 815, 823-26 （2012）

（processor）的定義，包括「自然人、法人，公務機關（構）或其他組織（natural or legal person, public authority, agency or other body）」[3]。

3. 保護客體

歐盟個人資料規則之保護客體為「任何有關已被識別（identified）或可被識別（identifiable）之自然人的資料」。依據歐盟個人資料規則第 4 條定義，所謂「可被識別的自然人」係指：可以透過識別符（identifier），例如：姓名、識別號碼、位置資料（location data）、線上識別符（online identifier），或經由其他一或多項身體、生理、基因、精神、經濟、文化或社會身分特徵，直接或間接識別的自然人[4]。其中，規則並未定義「位置資料」，而「線上識別符」係指由裝置、應用程式、工具或網路協定所賦予的唯一識別符，例如：網路協定位址（internet protocol address）等其他識別符，例如：無線射頻識別標籤（Radio Frequency Identification tag）[5]。GDPR 則將位置資料與線上識別符視為「可被識別」的個人資料。

3 GDPR Article 4（7）,（8）.
4 Article 29 Data Protection Working Party Opinion 4/2007 on the concept of personal data
5 GDPR Recital 30.

4. 適用範圍[6]

1995 年資料保護指令適用屬地原則，如果企業提供跨境服務，但未於歐盟地區設立組織，則不適用資料保護指令。依據 GDPR 第 3 條規定：即使資料控制者未於歐盟境內設立組織，但跨境提供商品或服務時，蒐集處理歐盟居民個人資料，則適用 GDPR 規範，並須在歐盟境內指派特定代表負責法令遵循事宜。

5. 資料處理原則[7]

資料控制者處理個人資料應當合法、正當、透明，以明確特定目的蒐集，僅處理達到目的之最小化資料，並應保持資料完整與準確，儲存資料期限不得超出達到目的所需時間，同時採取技術與管理措施確保資料安全性。

6. 合法處理個人資料[8]

處理個人資料應符合法定要件之一，包括當事人同意為特定目的處理資料、履行契約所需、維護公共利益或行使政府授予的權力、保護當事人或其他自然人的重要利益等，才能處理當事人資料；其中當事人同意，定

6 GDPR Article 3
7 GDPR Article 5
8 GDPR Article 6

義為個人資料當事人在被告知之前提下，依其自由意願所作出具體明確同意其資料被處理的意願。

7. 個人資料揭露通報[9]

若對個人資料當事人的權利或自由有重大危害之虞時，資料控制者必須毫不延誤地（without undue delay）通知個人資料當事人，並應於 72 小時內向資料保護主管機關（Data Protection Authority）報告個人資料的揭露情況

8. 不同意權

於特定情況下，個人資料當事人有權不同意資料被處理，除非資料控制者能證明處理該資料有重大正當理由，優先於個人資料當事人之基本權利與自由。當個人資料當事人提出不同意時，資料控制者應立即停止處理該個人資料。不同意權亦適用於以大量個人資料所自動化產生之「描繪（profiling）」活動，亦即個人資料當事人有權瞭解特定服務是如何決策，包括以巨量資料為基礎，運用機器學習、人工智慧技術進行資料分析與研判的服務，例如 Facebook。

9 GDPR Article 33, Article 34

9. 被遺忘權[10]

當個人資料與蒐集處理之目的無關、個人資料當事人不希望其資料被處理或資料控制者無正當理由保存該資料時，個人資料當事人得要求資料控制者刪除所蒐集的個人資料。若該資料傳送給合作第三方，資料控制者應通知該第三方刪除該資料。

10. 資料可攜權[11]

個人資料當事人可向資料控制者索其資料，也可將其個人資料轉移至另一個人資料料控制者。歐盟公民能擁有本身個人資料的操控權，包括「資料可攜權」，例如：用戶可以將其個人資料以及其他相關資料從一社群網路移轉至另一社群網路。

11. 資料保護影響評估[12]

GDPR 要求企業必須進行「資料保護衝擊評鑑（Data Protection Impact Assessments, DPIA）」[13]，以敘明業務活動中涉及個人隱私權的風險，並加以衡量、管理與因應，並於蒐集與處理個人資料前，評估該等風險與

10 GDPR Article 17
11 GDPR Article 20
12 GDPR Article 35
13 Article 29 Data Protection Working Party, WP248, Guidelines on Data Protection Impact Assessment （DPIA） and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679.

業務活動之必要性。

12. 設置資料保護長[14]

GDPR 要求企業員工達一定規模以上，且業務涉及歐盟居民的個人資料處理，將強制要求資料控制者與資料處理者設置資料保護長（Data Protection Officer, DPO），以確保企業對資料保護遵循性，並處理資料保護相關事務，同時承擔 GDPR 法律責任。

13. 罰款[15]

對於一般性的違法，罰款上限是 1,000 萬歐元或企業前一年度全球營業收入的 2%（兩者取金額高者）；對於嚴重的違法，罰款上限是 2,000 萬歐元或企業前一年度全球營業收入 4%（兩者中取金額高者）。

(二) 電子隱私指令

1. 背景

因應網際網路與傳統通訊網路的差異，且為廣大範圍的電子通訊服務提供一個共同及全球性的基礎設施。以網際網路提供公共使用之電子通訊

14 GDPR Article 37, 38, 39
15 GDPR Article 83

服務，已對個人資料與隱私產生新的風險，特別是網際網路之個人資料與隱私權的保護相關議題。鑑此，2002 年，歐洲議會與歐盟理事會通過電子隱私指令（E-Privacy Directive），針對公眾通訊網路，特別是用戶個人資料自動儲存與處理能力部分，提供法律、管制政策與技術上的特別規定，確保法人與自然人之基本權利及自由能得到妥善保護。

2. 規範主體、行為與客體

此指令適用之主體為在歐盟境內提供公眾使用之電信服務業者；規範歐盟境內利用公眾通訊網路、封包交換網路及網際網路中關於電子通訊服務之個人資料處理行為，客體包含用戶與使用者之通訊資料、位置資訊等，並將法人的資料亦納入保護範圍。

(1) 訊務資料（Traffic data）[16]

訊務資料係指以電子通訊網路中通訊傳輸為目的、或為歸責（Accountability）目的而處理的資料。此等由公眾通訊網路或公眾電子通訊服務提供者所處理及儲存，與用戶相關之訊務資料，當其通訊傳輸的目的消失時，必須刪除或去識別化處理[17]。此外，為行銷電子通訊服務或提供

16歐盟，Directive 2002/58/EC，Article 2（b），「"traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof」。
17歐盟，Directive 2002/58/EC，Article 6.1。

加值服務[18]之目的，應取得用戶同意，公眾電子通訊服務提供者得於目的之必要範圍及期間內處理訊務資料，且亦應提供用戶撤銷同意之機會[19]。

(2) 位置資料（Location data）[20]

位置資料係指於電子通訊網路中處理、得以識別公眾電子通訊服務使用者的終端設備所在地理位置，例如：用戶終端設備之經度、緯度與高度等。位置資料亦可能提供加值服務所需資訊，例如：提供駕駛個人化的交通資訊與駕駛方向。公眾通訊網路或公眾電子通訊服務提供者處理此等位置資料，只能經去識別化或取得用戶同意後，在加值服務之必要範圍及期間內進行處理，且服務提供者必須於取得同意前，告知用戶下列相關事項：

- 欲處理的位置資料種類；
- 處理的用途與時段；
- 提供該加值服務時，位置資料是否會傳輸至第三方。

此外，取得用戶對處理位置資料同意後，亦須讓用戶能隨時撤銷同意，或暫時拒絕位置資料的處理。同樣地，第三方授權之人員僅能於加值服務之必要範圍內處理位置資料。

18加值服務係指任何基於通訊服務，且須利用當事人通訊資訊或位置資訊的服務
19歐盟，Directive 2002/58/EC，Article 6.3。
20歐盟，Directive 2002/58/EC，Article 2（c），「"location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service」。

3. 近期發展

2017年,歐盟委員會提出將電子隱私指令升級為電子隱私規則的提案，使其與 GDPR 要求一致，並期望能於 2018 年與 GDPR 同時生效。電子隱私指令自 2002 年實施後曾於 2009 年進行修訂，主要的修訂內容是針對用戶端設備所儲存訊錄（cookies），必須從選擇退出（opt-out）改為選擇加入（opt-in）。此次，歐盟委員會提案主要修訂要點如下：

(1) 擴增電子通訊服務定義

修訂電子通訊服務定義，包括：

- 網際網路接取服務（Internet Access Service）

  無論所使用的網路技術與終端設備為何，能提供網際網路接取與連結網際網路端點的公眾電子通訊服務。

- 人際通訊服務（Interpersonal Communications Service）

  人際通訊服務：指具備人際交往與互動溝通功能的通訊服務，亦涵蓋被納入於主要服務的輔助功能服務。因此將包括 IP 電話、簡訊服務、網頁郵件服務與 OTT 等服務。例如：具備玩家溝通功能的網路遊戲，亦算是人際通訊服務。

- 電子通訊網路傳輸訊號的服務（services consisting wholly or mainly in

the conveyance of signals on electronic communications networks）

指傳統的電信服務、機器間的訊號傳輸服務（機器與機器間的通訊）、廣播服務。此次歐盟委員會專門針對 IoT 時代，提供機器對機器通訊隱私與機密性的保護。依照定義瀏覽網際網路，存取具體網站或網頁亦會被認為是一種電子通訊，因為個人與網站、網頁與網頁間存在資料傳輸，因此亦是電子通訊。只要電子通訊服務不具備公眾特性，則可不適用電子隱私規則，例如不公開的企業內部通訊服務。

(2) 適用範圍

適用於電子通訊服務業者、公開名錄業者（directories），以及提供電子通訊的軟體業者，包括網際網路上檢索與提供資訊者，亦適用於使用電子通訊服務直接行銷商業通訊或蒐集與用戶終端設備有關資訊的自然人與法人，依照規定只要在歐盟提供相關服務，即使非歐盟國家的業者，均須於歐盟派駐代表。

(3) 訊錄同意機制

若用戶網路瀏覽器上的隱私設置已設定為同意，則網站營運者投放行為定向廣告時，可不需向用戶徵求同意使用訊錄（cookies）。

(4) 電子通訊保密

確保各方交流的資訊，包括隨時隨地發送資訊，通訊內容不會被揭露。保密性將包括兩個面向：內容與詮釋資料（meta data），因為詮釋資料亦涉及個人資訊與隱私，例如：撥打過的電話、瀏覽的網頁、地理位置、發話時間、日期與時段。主要的保密原則為未經同意（consent），不能干擾電子通訊，不得截取、儲存、使用電子通訊的資料。值得注意的是，與 GDPR 只保護自然人不同，電子隱私規則亦將法人的通訊列入保護範圍，因此當電子通訊的終端用戶為法人時，GDPR 的部分規定，特別是關於徵求「同意」的要求，同樣適用。

(三) 去識別化機制

1. 歐盟個人資料保護規則

GDPR 並未正式定義不可復原的「匿名資訊（anonymous information）」，但其條文對規則未規範的「非」個人資料有較指令更為明確說明。第 26 條提到去識別化處理，並規定該規則不適用於去識別化處理的資料：

- 鑒於資料保護原則必須適用於與身分已確定或可確定的與個人有關之任何資訊；
- 鑒於在確認當事人身分是否可識別時，應考慮負責處理個人資料的實體或任何其他人為了識別該當事人身分從而可能採取之一切合理

可行方法；

- 鑒於資料保護原則不適用於以去識別化處理，以致無法識別資料當事人身分的資料。

具體而言，第 26 條定義去識別化技術，強調以去識別方式處理任何資料時，必須充分除去當中的重要元素，防止當事人的身分被識別。亦即處理資料的方式讓無論是資料蒐集者或是第三方透過“採取一切合理可行的方法，均無法識別特定自然人的身分”，而其中的一個重要元素為處理結果是不可逆的。

GDPR 並未明確規定應該或如何進行去識別化處理，而係著重於處理結果，亦即無法透過一切、可行與合理的方法重新識別資料當事人。故此，行為守則中明訂的去識別化處理機制和資料保留形式，均須為“不再可能”重新識別資料當事人的資料。若資訊符合上述定義，則可不適用個人資料保護的各項規則；即便為統計或研究目的使用此等不可復原的去識別化資料，亦不屬歐盟個人資料規則的規範範圍。

2. 歐盟電子隱私指令

歐盟電子隱私指令定義之相關去識別化規範包括：

- 第 6 條第 1 款中規定：經公眾電信網路或公眾電子通訊服務業者處

理並儲存的資料，如屬於與登記戶和用戶相關的訊務資料，當不再需要用於通訊傳輸目的時，須刪除或匿名。

- 第 9 條第 1 款規定：如資料屬於位置資料以外的訊務資料，且與公眾通訊網路或公眾電子通訊服務的用戶（user）或訂用戶（subscriber）有關時，只有當資料被去識別化以後才可以被處理，又或用戶或訂用戶對為提供增值服務所必需的範圍和期間曾經表示同意，則有關資料亦可以被處理。
- 第 26 條：用於銷售通訊服務或提供增值服務的訊務資料，應於提供服務後，須刪除或匿名。

此等條文的立法原意在於針對適用於個人資料的去識別化處理技術，以目前的科技而言，應能產生等同刪除之永久性結果，亦即使個人資料不可能再被處理[21]。

(四) 去識別化技術意見書

歐盟第 29 條資料保護工作小組於 2014 年 4 月通過去識別化技術意見書，該意見書針對不同去識別化技術提出評估資料是否已達去識別化的 3 項基本條件，分別為：

21國際標準 ISO 29100 之去識別化定義：“對可識別個人身分資訊（PII）進行不可逆轉的修改過程，使 PII 的資料蒐集者無法單獨地或與任何其他方合作，直接或間接識別 PII 主體身分”（ISO 29100:2011）。因此與第 95/46 號指令的原則和概念相同，適用某些國家法律中的定義（如義大利、德國和斯洛文尼亞），這些國家的法律都聚焦在不可識別性（non-identifiability）。然而，法國的資料保護法律規定，即使再識別資料當事人的身分是極其困難甚至是不可能，資料仍然屬於個人資料。換言之，法律並沒有“合理性”測試（“reasonableness” test）的規定。

- 是否仍可唯一辨識某個個人；
- 是否仍可關聯到某個個人紀錄；
- 是否能推斷出與某個個人有關的資訊。

該意見書中指出各種去識別化技術都有其優點、缺點，資料蒐集者對於個人資料的利用需求不同，資料集合亦存在差異，去識別化技術與設定參數難以有統一的標準。其次，各種去識別化技術亦無法能完全達到避免「重新識別」的殘餘風險（residual risk）。事實上，就算個案已無法復原某資料當事人的紀錄，但仍有可能借助其他資訊來源（不論是否公開）蒐集與該個人相關的資訊。此外，去識別化處理過程亦會對資料當事人帶來直接影響（由於當事人事前未知悉被包含在分群中，或未因此而給予事前同意，因而覺得惱怒、浪費時間以及失去資訊自主權），更有可能遭受其他間接影響。例如：若當事人被誤列為攻擊目標，尤其是惡意攻擊的話，當事人經去識別化的資料便可能被重新識別。因此，僅於去識別化技術與先決條件（全景）、目的已清晰界定時，方能產生良好的去識別化效果。

意見書中指出資料蒐集者欲使用某種去識別化技術前，應仔細規劃去識別化處理的過程細節，包括去識別化的目的、公布資料集時能否保護個人隱私，以及攻擊者能否從公開的資料集獲取特定資訊。針對去識別化的 3 項基本要求，表 3 列舉不同去識別化技術的優缺點。

表 3、去識別化技術優點

	是否仍然存在被挑出的風險？	是否仍然存在關聯風險？	是否仍然存在推論風險？
假名化（pseudonymisation）	是	是	是
添加雜訊（noise addition）	是	不太會	不太會
替換（substitution）	是	是	不太會
聚合或K-匿名（aggregation or K-anonymity）	否	是	是
L-多樣性（L-diversity）	否	是	不太會
差分隱私	不太會	不太會	不太會
雜湊化/符記化 hashing/tokenization）	是	是	不太會

資料來源：European Commission, Opinion on Anonymisation Techniques

最佳解決方案應視個案而定，依據比較分析，除採取可行的資料去識別化處理程序與技術外，亦應全面評估去識別化風險。若法律明訂監理機關須評估去識別化過程，則資料蒐集者應向監理機關提交評估結果。為降低重新識別之風險，資料蒐集者可考慮以下的去識別化方案：

1. 不採用“發佈後遺忘”（Release and Forget）模式，考量重新識別殘餘風險，資料蒐集者應：

- 定期評估是否存在新的風險，重新識別殘餘風險；
- 對於已確定風險，評估採取的措施是否足夠，並相應調整；
- 監控風險。

2. 針對殘餘風險，特別考量資料集是否存在非去識別化的部分與已去識別化的部分兩者組合時，是否會發生重新識別，以及屬性之間是否存在關聯（如位置與財務資料）。

二、 美國

對於個人資料保護，美國尚未有一體適用之個人資料與隱私權保護規範，僅由不同產業領域訂定不同的規範，以下舉列與本計畫相關之法規說明。

(一) 有線電視通訊政策法（Cable Communications Policy Act）

1984 年，美國國會訂定有線電視通訊政策法，該法規範有線電視業者蒐集、利用與揭露用戶個人資料之保護規則。1992 年，國會另訂定有線電視消費者保護暨競爭法（Cable Television Consumer Protection and Competition Act），該法係屬聯邦法規，將個人資料定義為可被識別個人身分的資料，不包括無法識別之特定個人之總合統計資料[22]，規範對象為有線電視業者（Cable Operator），係指經營管理有線電視系統以提供有線電視服務的業者，亦包括有線電視業者所有、控制或共有，以及提供有線或無

22 'personally identifiable information' does not include any record of aggregate data which does not identify particular persons; Cable Television Consumer Protection and Competition Act of 1992 , Sec. 20. Customer Privacy Rights.

線通訊之其他服務者[23]。而「其他服務」包括利用有線電視業者設備提供的有線或無線通訊服務[24]。

1. 通知用戶

有線電視業者須善盡告知用戶對於其個人資料蒐集、利用、處理的義務，在簽訂有線電視服務或其他服務協議時，有線電視業者應每年至少一次以分別及書面的形式通知用戶以下事項：

- 所蒐集個人資料的性質與用途；
- 資料揭露的方式、次數與目的；
- 有線電視業者維護保存資料的時限；
- 用戶可存取此等資訊的時間與地點；
- 本條款規定蒐集、揭露個人資料之相關限制與本條款賦予用戶的權利[25]。

2. 蒐集個人可識別資訊

有線電視業者除為提供有線電視服務或其他服務給用戶，或是為偵測

23'cable operator' includes, in addition to persons within the definition of cable operator in section 602, any person who （i） is owned or controlled by, or under common ownership or control with, a cable operator, and （ii） provides any wire or radio communications service."; Cable Television Consumer Protection and Competition Act of 1992 , Sec. 20. Customer Privacy Rights.

24 'other service'.includes any wire or radio communications service provided using any of the facilities of a cable operator that are used in the provision of cable service; Cable Television Consumer Protection and Competition Act of 1992 , Sec. 20. Customer Privacy Rights.

25 47 U.S.C. 551

未經授權之收視情形得蒐集用戶個人資料外，欲利用有線電視系統蒐集用戶個人資料，均須事先取得用戶經書面或電子形式表示之同意[26]。

3. 資料揭露

有線電視業者原則上必須事先取得用戶經書面或電子形式之表示同意，方能向第三方揭露用戶個人資料。於下述情況下，業者得不經用戶同意，揭露用戶個人資料[27]：

- 為提供有線電視服務或其他服務之目的；
- 依循法院命令，向政府單位提供用戶個人資料；
- 業者應於賦予用戶機會限制或禁止揭露行為之後，揭露用戶姓名與住址予其他有線電視服務或其他服務業者，且此種揭露行為無法直接或間接顯示該用戶收視習慣或該用戶在有線電視系統上的交易種類。

4. 用戶存取資訊

有線電視用戶應具有對其個人資料存取之權利，有線電視業者應於適當時間及地點提供用戶存取其個人資料，包括用戶更正資料的機會[28]。

26 47 U.S.C. 551（b）
27 47 U.S.C. 551（c）
28 47 U.S.C. 551（d）

5. 資料銷毀

若當初蒐集資料的目的已不存在，且無保留資料之必要性，或是無用戶請求存取此等資料時，有線電視業者應銷毀此等用戶個人資料[29]。

(二) 電信法

1996 年，美國通過修訂電信法（Telecommunication Act），於其第 222 條針對電信事業個人資料隱私訂定相關規範，旨在保護電信業者、設備製造商、用戶相關資訊之隱密性。與本計畫相關的規範客體與規範行為說明如下：

1. 客戶專線網路資料（Customer proprietary network information, CPNI）

CPNI 係指「電信事業用戶基於電信服務契約而使電信事業取得有關使用電信服務數、技術規格、型態、目的地與總額之資訊」，亦包括「客戶資訊相關的電話服務帳務資訊」，通常即為電信事業為提供服務時由用戶取得的資訊。

除法律規定或為提供服務，以及公共利益考量或經客戶同意之外。電信服務業者僅能在提供：

29 47 U.S.C. 551（e）

- 蒐集該資訊之特定電信服務或；
- 其他必要的相關服務（包含發行名錄）始得利用、揭露，或准許存取此類資料。

2. 位置資訊

CPNI 定義亦包括用戶位置資訊，規定必須事先取得客戶明示授權使用無線位置資料（Wireless Location Information），位置資料包括：

- 有關商業行動裝置服務的通話位置資訊；
- 自動當機時所通知的資訊。

3. 聚合統計資訊（Aggregation Information）

聚合統計資訊係指關於群體、或服務或客戶類型的集合資料，其用戶個人的身分與特徵已被移除。相較於 CPNI，聚合統計資料已缺乏個人特徵辨識度，對於個人隱私的影響較小，然而此類資料常用於競爭市場分析。依規定電信服務業者因提供電信服務而取得客戶 CPNI 者，得使用、揭露、允許存取利用客戶的總合統計資料，而不受限於前述有關 CPNI 規範[30]。

(三) 寬頻服務之用戶隱私保護

2015 年 5 月，聯邦通訊傳播委員會對寬頻服務的 ISP 業者發佈保護用

30 47 U.S.C. 222（c）(3)

戶隱私執行建議（FCC Enforcement Advisory），後又於同年 11 月表示將儘速針對寬頻業者保護用戶隱私制定規範並發佈制定命令公告（Notice of Proposed Rulemaking）。2016 年 10 月聯邦通訊傳播委員會通過網路中立性隱私法案，主要保護消費者在非允許的情況下，網際網路服務提供者（Internet Service Provider, ISP）不得販售用戶個人資料，政策主要有以下規範：

- ISP 業者須主動通知用戶將蒐集哪些類型資料，以及此等資訊會傳送給何人？
- 以確保用戶個人資料安全為前提，提供用戶勾選同意傳送哪種類型資料，例如：理財、健康；
- 意外洩漏資料時，應即時通知用戶。

該法案原先預計 2017 年底實行，但美國參議院於 2017 年 3 月 23 日以些微票數差距未通過此項法案，此一決議仍待美國眾議院審核。

(四) 去識別化機制

2015 年，美國國家標準技術研究院（National Institute of Standards and Technology, NIST）公布個人資訊去識別化研究報告（NISTIR 8053）。該報告指出藉由公開資料分享可提升政府行政效能，並提供產業界新資源。然而，資料可能包含可識別之個人資訊，例如：姓名、email 帳號、地理定位

資訊或照片，形成資料利用目的與個人隱私保護間之衝突。當組織編製、利用、歸檔、分享及公開含有個人資料之資料，透過去識別化技術可移除個人敏感資訊，降低個人隱私風險，平衡資料利用與個人隱私保護間的衝突。其次，去識別化資料於蒐集後經最小加工處理，可降低資料利用與歸檔之成本，降低資料外洩之隱私風險。

美國已有多項法規支持去識別化做法，包括教育部支持家庭及學業紀錄隱私法、醫療保險可攜性與責任法（Health Insurance Portability and Accountability Act, HIPAA）等方面，在不公開個人資料當事人身分下，保留資料可用性，不受法律限制。

抑制（suppressing）或概化（generalizing）資料庫特定屬性之去識別化方法，並無法絕對保證隱私，因為仍有可能利用輔助資料集（auxiliary dataset），依殘餘資料重新識別當事人。由於存在重新識別風險，有些組織分享去識別化資料時，會要求資料使用者簽署資料使用協議，例如：資料使用協議可能禁止已去識別資料接收者試圖重新識別當事人、連結外部資料或未經同意下分享資料。

1. 個人資料使用保護模式

學界對使用資料庫個人資料之隱私保護，發展出兩種模式：

- 隱私保護資料探勘（Privacy Preserving Data Mining, PPDM）

  此模式不釋出原始資料，而係用以供統計處理或機器學習[31]。運算處理結果之呈現，可能以經加總或聚合後之統計圖表、機器學習程式（Machine Learning Algorithms）加以分類，及其他類型的結果等方式表達。

- 隱私保護資料公開（Privacy Preserving Data Publishing, PPDP）

  在此模式下，原始資料經過處理，產生一種新的去識別化或聚合資料（synthetic data）產出，以供使用者利用。

兩種模式皆具「隱私保護作用」，即僅釋出部分資訊（例如：聚合資訊、統計結果、分類或合成數據），而不公開原始資料集內，可識別特定個人的資訊。所謂統計資料揭露限制（statistical disclosure limitation），指修改統計資料，以防範第三者利用該統計資料識別個人。揭露限制技術包含：分類概括、擾亂資料與雜訊添加。

31 機器學習是一種電腦運算程式及技術，由電腦內部程式加以分類資訊，並識別數據內之規律。

2. 去識別化資料流向模式

去識別化流程如圖 3 所示。原始資料之蒐集源自「個人資料當事人(data subject)」，將個人資料彙集為「含個人資訊的資料集」，經去識別化後另形成未具識別性的新資料集。該新資料集可供組織內部使用，以降低隱私風險；亦可供值得信賴的資料接收者（trusted data recipients）使用，該資料接收者受行政管理約制，例如：資料使用協議。於此種情況中，所要求之去識別化程度較低。此外，新資料集可能供未知的大眾使用，例如：公開去識別化資料於網際網路，此時因被重新識別之風險較高，故所要求之去識別化程度較高。

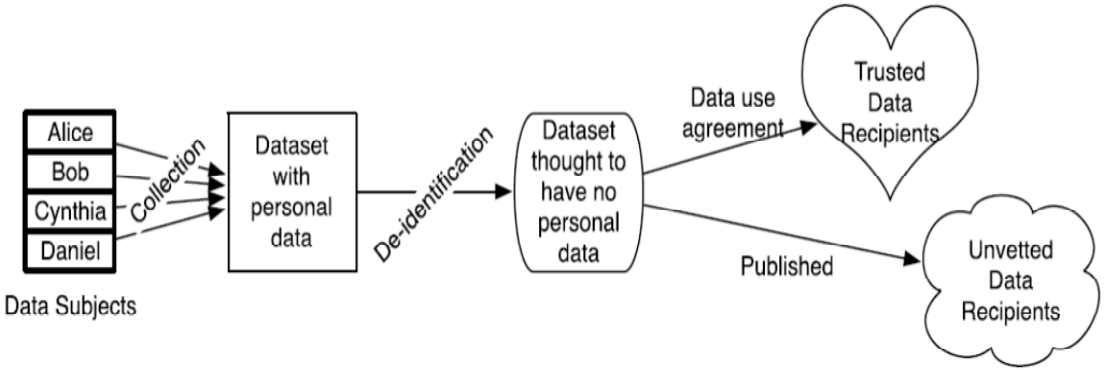

圖 3、資料蒐集、去識別化及利用

資料來源：NIST, De-Identification of Personal Information

3. 重新識別身分攻擊與不當侵入者

重新識別身分，指試圖在已去識別化資料中識別當事人之方法。去識

別化之主要目的，在於防範未經許可的重新識別當事人；此種未經許可地試圖重新識別當事人，稱為重新識別攻擊[32]。個人或組織試圖重新識別當事人的主要原因如下：

- 測試去識別化資料之品質；
- 博取公眾名聲或專業地位；
- 傷害公布已去識別化資料組織之名聲；
- 獲取重新識別當事人資料之直接利益；
- 為中傷特定當事人，例如威脅、勒索等負面做法。

至於重新識別之風險，係指資料集內個人的個別識別符與其他資料，可由去識別化資料中獲知之風險程度。量化此風險相當複雜，須視原始資料集、去識別化技術、攻擊技術功力、攻擊者所擁有資源，以及是否有連結去識別化資料的額外資料等因素而定。於公布經去識別化資料後，重新識別之風險將與日俱增，因為技術精進與可利用的脈絡資訊日增（例如：資訊公開或購買資訊），且不太可能有可檢測所有脈絡資訊的演算法或技術。

4. 資料釋出模式與管控方法

管控資料取得與利用為防範重新識別身分的方法之一，依資料釋出方

32 Ibid, p.9-para.4.

式之不同，主要有下列三種：[33]

- 發佈後遺忘（Release and Forget）模式

  去識別化資料一旦釋出於大眾，例如發布於網際網路，資料可能難以回收，甚或不可能回收。

- 資料使用協議（Data Use Agreement, DUA）模式

  去識別化資料可在具法律約束力的資料使用協議下提供，詳細列示資料使用之可為與不可為。資料使用協議通常禁止已去識別資料接收者試圖重新識別身分、連結其他資料或分享資料。資料使用協議的型態有二：「適格研究員模式（qualified investigator model）」，指資料擁有者與符合資格研究人員間協商資料使用協議；「點擊模式（click-through model）」，僅簡單於網際網路下載資料前，點擊同意協議內容。

- 飛地（Enclave）模式

  經去識別化資料儲存於經隔離的飛地，以限制原始資料外流，僅接受符合資格研究人員之查詢、在去識別化資料中執行搜尋，及回覆查詢結果。

33 Ibid, p.14-para.1.

5. 個人資料去識別化及重新識別方法

(1) 移除直接識別資料

直接識別資料（direct identifier），亦稱為直接識別參數或直接識別符，係指可直接識別個人的資料。例如：姓名、身分證統一編號及 email 帳號。依 ISO/TS 25237:2008（E）之定義，所謂直接識別資料，指在無額外資訊或經交叉連接公共領域（public domain）資訊下，可直接識別至個人的資料。並建議將其他個人化資訊，例如：醫療紀錄號碼及電話號碼，視為直接識別資料，即使尚需額外資訊始可連接個人，因為此種型態的識別資料經擴大運用，將可識別個人。

另依美國醫療保險可攜性與責任法（HIPAA）之定義，直接識別資料共有 18 項，包含姓名、電話號碼、email 帳號及其他號碼、特性或代碼等。對於去識別化，直接識別資料須予以移除或轉化。早期去識別化之作法，止於移除直接識別資料，致使殘存資料可能經由連結攻擊而遭重新識別。

(2) 假名化

假名化亦稱擬匿名化，係一種特殊轉化，將姓名及其他可直接識別個人之資訊，以假名取代。在全部直接識別資料採系統化作假名之情況下，假名化仍可使歸屬於個人的多種資料紀錄或資訊系統被連結。執行假名化

的組織通常儲存真假名對照表，或以演算法代換，若對照表或演算法遭破解，假名化可能很容易遭逆向推敲。

況且即使未保存真假名對照表，於多個人資料料集中一致地使用相同假名之情況下，很容易遭受連接攻擊。基此，歐盟執委會資料保護第 29 條工作小組指出，「假名化資料不等於匿名資料，因為假名化資料，經不同資料集交叉比對，仍可能遭識別。」然而，由於假名化降低原始身分之連接性，但假名化仍不失為「有效的安全措施」。

(3) 以連接攻擊重新識別

另一種重新識別經去識別化資料集之方法，為連接攻擊（linkage attack）。於此種攻擊下，已去識別化資料集內每項紀錄，可連接至另一類似資料集（此處稱為第二資料集），兩者間存在可連結資訊，且該第二資料集含有可識別身分的資料。

(4) 準識別符之去識別化

所謂準識別符（quasi-identifier），亦稱為間接識別符或間接識別變數，指該識別符本身無從識別個人資料當事人，然經與其他資訊聚合或「連接」後，可識別當事人。例如：聚合出生日期、郵遞區號及性別等資訊，通常可識別特定當事人。

準識別符之去識別化極具挑戰，直接識別符可自資料集移除；而準識別符可能隱含對未來分析的重要資訊，消除準識別符，可能影響該資料集之實用性。去識別化準識別符之方法，主要為藏匿、概化、資料擾動（perturbation）、排列變更（swapping）及局部抽樣（sub-sampling）等。

k 匿名為準識別符去識別化方法之代表，該方法係植基於等價類別（equivalence class）之概念，即匹配其全部準識別符值的紀錄組。宣稱符合 k 匿名的資料集，其中各準識別符組合，須至少具有 k 筆相對應紀錄。例如：資料集包含出生日期與出生地等資訊，有 k＝4 匿名，則每個紀錄組至少有 4 筆相同結合出生日期與出生地的紀錄，可達到既定程度之隱私性。

(5) 醫療保險可攜性與責任法下受保護醫療資訊之去識別化

依 1996 年醫療保險可攜性與責任法之規定，關於隱私方面，明定 2 種受保護醫療資訊去識別化方法，說明如下：

- 專家確定法（Expert Determination Method）

  所謂專家確定法，係指由專家檢視資料，並確定去識別化方法，以最小化重新識別身分之風險。由具備專門學識及經驗，並經適當統計和科學原則與方法專業訓練者擔任。（第 164.514 條第 b 項第 1 款）

  ✓ 在單獨或結合其他合理現有資訊下利用該資訊，確定由可預期接收

者重新識別當事人之風險相當低。

✓ 記錄目前確定之方法與其分析結果之證據。

- 安全港法（Safe Habor Method）

安全港法指出去除資料中個人及其親屬、雇主或家庭成員之資訊，即為已去識別化之方法。相關資訊如下：

✓ 姓名；

✓ 電話號碼；

✓ 傳真號碼；

✓ email 帳號；

✓ 社會安全號碼；

✓ 就醫紀錄號碼；

✓ 醫療保單受益人號碼；

✓ 銀行帳號；

✓ 證照號碼；

✓ 駕照識別符及序號，含車牌號碼；

✓ 裝置識別符及序號；

✓ 網站（URL）位址；

✓ 網際網路協定（IP）位址；

✓ 生物辨識，含指紋及聲紋；

✓ 全臉部照片及任何可區別影像；

✓ 其他唯一識別符、特徵或代碼。

三、 英國

(一) 個人資料保護法

1. 背景

英國於 1984 年及 1987 年分別公布「資料保護法」（Data Protection Act 1984, DPA）與「個人檔案使用法」。其後為配合歐盟 1995 年實施之個人資料保護指令 95/46/EC，遂於 1998 年通過現行之資料保護法（The Data Protection Act 1998），自 2000 年 3 月生效，規範國內所有涉及個人資料之蒐集、處理、利用之行為。該法將保護客體由經電腦處理之個人資料延伸到特定形式之人工資料[34]，「處理」一詞之內涵亦被擴大，包含取得、儲存、利用與揭露個人資料[35]，因此在上述對於保護客體的定義下，大部分形式的個人資料已納入保護範圍。該法並增列，在一般情況下，必須取得個人資料當事人同意以及對跨國界個人資料傳輸活動加以規範的原則。

34 Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. Note that this definition extends the Act to include manual files which contain information about an individual, such as personnel files. Data Protection Act of 1998 （Interpretation）.

35 Obtaining, recording or holding the data or carrying out any operation on the data, including organising, adapting or alteration of the data; retrieval, consultation or use of the data; disclosure of the data, and alignment, combination, blocking, erasure or destruction of the data. If in doubt, assume that it is processing. Id.

2. 個人資料定義

個人資料定義僅涉及活著的人，一旦該人死亡，個人資料保護法所保障的權利隨即終止。其次，定義僅限於自然人，而法人非規範範圍。第 1 條第 1 款規定資料涉及（related to）個人，始得個人可經由資料而識別，或經由資料在配合同一位資料控制者（data controller）所擁有或即將擁有之其他資訊而識別。舉例說明如下：

- 某資料庫中，儲存某公司名稱與該公司員工姓名，該兩筆資訊即屬個人資料，因該個人可經由姓名及工作地點被識別；
- 當一資料管理者擁有 2 個資料庫，該 2 個資料庫的資訊結合後，可識別出某個人，即使個別檢視單一資料庫，無法識別該個人，但資料庫中資訊仍屬於個人資料。

3. 資料保護原則

資料保護法規範資料控制者於處理個人資料時應遵循 8 項原則[36]：

(1) 個人資料應被公平、合法地處理，特別是，若未滿足以下條件，則不能進行處理。

- 至少滿足以下條款之一：
  - ✓ 處理係已經個人資料當事人（資料被儲存的人）同意（許可）；

36英國，個人資料保護法，Schedule 1。

- ✓ 處理係執行或開始契約所必需；
- ✓ 處理係因應（於契約規定外）法律上義務所必需；
- ✓ 處理係保護個人資料當事人的切身利益所必需；
- ✓ 處理係促進任何公共利益所必需；
- ✓ 處理係「資料控制」或「第三方」追求合法利益所必需（除非此舉可能損害個人資料當事人的利益）。

(2) 個人資料取得應依據於一或多個明確規定。

(3) 處理個人資料應充分、與目的相關且不應超出目的所需。

(4) 個人資料應準確，並於必要時保持更新。

(5) 個人資料保存期限不得超過目的所需之保存期限。

(6) 關於個人權利，例如：個人資料將遵循個人資料當事人的權利處理。

(7) 應採取適當技術與組織措施，保護個人資料，防止未經授權或非法的處理個人資料，以及防止意外遺失、破壞或損壞個人資料。

(8) 個人資料不得轉移到歐洲經濟區以外的國家或地區，除非該國家或地區對有關個人資料處理方面確保個人資料當事人的權利和自主受到適當程度的保障。

4. 資料當事人權利

資料當事人權利係依循兩項原則而訂[37]：

37 David Bainbridge, Data Protection Law, 118 （2005）.

(1) 透明公開（Transparency）：為保障資料當事人權益，資料處理之相關資訊需透明公開，資料當事人有權瞭解資料管理者識別、蒐集與處理資料之目的，以及對誰揭露資料。

(2) 參與控制（Control）：資料當事人能參與控制資料處理之過程，提供資料當事人拒絕處理過程之權利。

為符合資料保護原則之目的，使資料當事人能瞭解其個人資料之蒐集與處理的相關資訊，並提供資料當事人參與資料處理過程之權利。資料保護法賦予資料當事人相關權利，包括：個人資料查閱請求權[38]；防止可能造成損害或不利的處理程序[39]；防止直銷[40]；防止自動化[41]；更正、封鎖、刪除、銷毀；損害賠償[42]。

5. 資料保護法管理架構

在英國資料保護法中，資訊長扮演主要執法角色，由該法賦予介入調查與執行法令之權利。資料控制者為決定資料蒐集目的與資料處理方法的人，需向資訊專員公署（Information Commissioner's Office）報備，並提供資料使用目的及處理方法等相關資訊，方可處理個人資料。資料處理者（data

38 英國，個人資料保護法，Section 7
39英國，個人資料保護法，Section 10
40英國，個人資料保護法，Section 11
41英國，個人資料保護法，Section 12
42英國，個人資料保護法，Section 14

processor）係指資料控制者依契約關係授權進行資料處理者，意即資料處理者經由資料控制者授權後，可代資料控制者處理資料。資料控制者具有向資料當事人告知相關資訊之義務，包括：個人資料如何蒐集、對誰揭露、處理資料目的為何？以及其他可確保資訊處理程序透明公正的資訊。當資料控制者欲將資料當事人的資料傳輸至第三國時，必須考量接收資料的國家是否有足夠的資料保護規範。

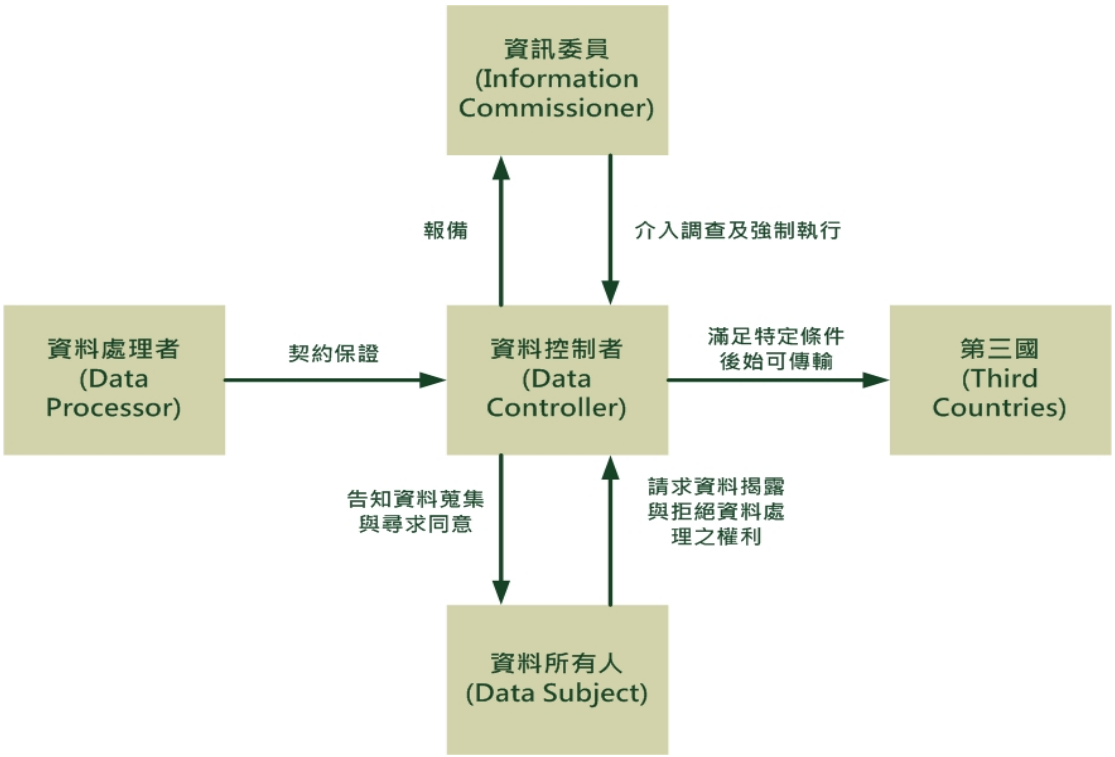

圖 4、英國個人資料保護法管理架構

資料來源：David Bainbridge, Data Protection Law 26

資料當事人對於可能造成損害之處理及直銷行為，具有拒絕之權利。意即個人資料處理過程須由資料當事人同意後始得運作（採 opt-in）。資料

當事人對其個人資料具有請求揭露之權利，並可針對不正確資料，要求更正、移除。此外，資料當事人亦具有防止直銷、防止自動化決定及要求損害賠償等權利。

(二) 隱私與電子通訊規則

2003 年，英國訂定隱私與電子通訊規則（Privacy and Electronic Communication Regulations, PECR），並於 2011 年修訂。該規則要求電子通訊服務提供者維護網路安全,告知用戶所承擔的風險與相對應之保護措施；並規範電子通訊安全中個人資料的蒐集、處理及利用。該規則強化現代人生活之個人通訊個人資料保障，亦可確保網路使用者撤回同意之自主權，若網路服務提供者未依規定善盡告知義務，則將面臨罰款。該規則同時亦賦予英國資訊專員公署稽核業者所蒐集網路使用者之網路使用行為資料，且得要求業者提供資訊。

1. 規範主體

適用對象為公眾電子通訊網路的用戶，包括自然人[43]、法人與非法人團體。規範對象以公眾電子通訊服務提供者（public communications service

43“Individual" means a living individual and includes an unincorporated body of such individuals. Id.

provider）[44]為主，公眾電子通訊服務提供者須提供確保網路安全的技術與組織措施，並要求通訊網路提供者（communications provider）[45]提供協助；此外若個人資料係由非服務提供者的第三方處理，則第三方資料處理者亦需納入規範。

2. 規範客體

規則將電子通訊服務中的資料區分為訊務資料、位置資料等類型。

(1) 訊務資料[46]

隱私與電子通訊規則主要沿用歐盟資料保護指令對於訊務資料之定義：以電子通訊網路中通訊傳輸為目的、或為歸責目的而處理的資料。但更進一步定義包括與通訊相關的發生時間、持續時間與路由資料。

服務提供者須取得個人資料當事人事前同意原則，在電子通訊行銷交易與訊務資料管理、客戶調查、詐欺預防與偵查、專為該用戶提供加值服務與電子通訊服務行銷的範圍內處理訊務資料。該規則第 7 條與第 8 條進一步說明資料處理原則：

44“Public communications provider" means a provider of a public electronic communications network or a public electronic communications service.” Id.
45“Communications provider" means a person who （within the meaning of section 32（4）） provides an electronic communications network or an electronic communications service.” Communications Act 2003, 2003 Chapter 21 section 405 （Intepretation）.
46https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/traffic-data/

- 服務提供者須告知用戶處理資料的相關資訊、目的與持續時間，且在公眾電子通訊提供者親為或在其監督下，可處理或儲存該個人資料當事人的訊務資料。
- 訊務資料須在處理期限內刪除或去識別化。

(2) 位置資料

位置資料通常與個人資訊具有較密切的相關性，規則要求經由提供服務的位置資訊，不得辨識個人資料當事人身分；或是在個人資料當事人同意且有必要之前提下，可將位置資料用於加值服務[47]。位置資料可由服務提供者親為，或在其監督下進行處理。在告知內容方面，服務提供者須告知個人資料當事人處理何種形式的位置資料、處理目的、處理期間以及該資訊是否會傳送給第三方處理。就個人資料當事人對於資料的自主性，個人資料當事人可隨時撤銷關於資料處理的同意，服務提供者須提供撤銷同意資料處理的便利方法，以強化個人資料當事人對個人資訊的自主性。

(3) 瀏覽歷程紀錄

依該規則，原則上不得於電信網路用戶之終端設備儲存或讀取資訊，例如：網站業者不得使用訊錄（cookies）技術追蹤網路使用者使用行為，除非可告知用戶訊錄存放位置、用途與儲存資訊，且取得其同意。用戶得

47 Value added service" means any service which requires the processing of traffic data or location data beyond that which is necessary for the transmission of a communication or the billing in respect of that communication.

透過設定網路瀏覽器之隱私選項或其他應用程式以表示同意（signify consent）。此外，若「發現個人資料遭侵犯時」可向主管機關英國資訊專員公署（Information Commissioner's Office, ICO）通報。

(三) 去識別化機制

依據資料保護法第 51 條[48]、第 52[49]條規定，英國資訊專員公署有義務推動資料控制者採取良好的資料保護做法，公署可與專業組織、研究單位與資料控制者與資料當事人諮詢後，提供實作業務守則，因此英國資訊專員公署於 2014 年公布去識別化實務作業規範[50]，作業規範並不限於資料保護法相關要求，同時符合歐盟資料保護指令規定，去識別化資料可不受資料保護法令之規範。該作業規範僅提供良好的實作建議，本身不具強制法律效力，可供資料保護法規範所屬組織參考，亦可以使用不同的方法實作，但須符合資料保護法的相關要求。ICO 不會對未實行良好實作的組織採取法律行動，亦不會依據作業規範提出的建議採取行動，除非其違反資料保護法。

48 http://www.legislation.gov.uk/ukpga/1998/29/section/51
49 http://www.legislation.gov.uk/ukpga/1998/29/section/52
50 ICO, Anonymisation: Managing Data Protection Risk Code of Practice, http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/anonymisation-codev2.pdf（last visited Apr. 16, 2014）.

1. 個人資料開放流程

公開資料的理由攸關如何進行公開，因為被識別出的風險與後果將有所不同：

- 依據資訊自由，以及政府公開法而進行之公開，係針對廣泛的網路世界，具有較高風險。
- 自行公開，諸如依研究目的或自身商業利益而進行之公開，較易控制與評估，但並非無風險。

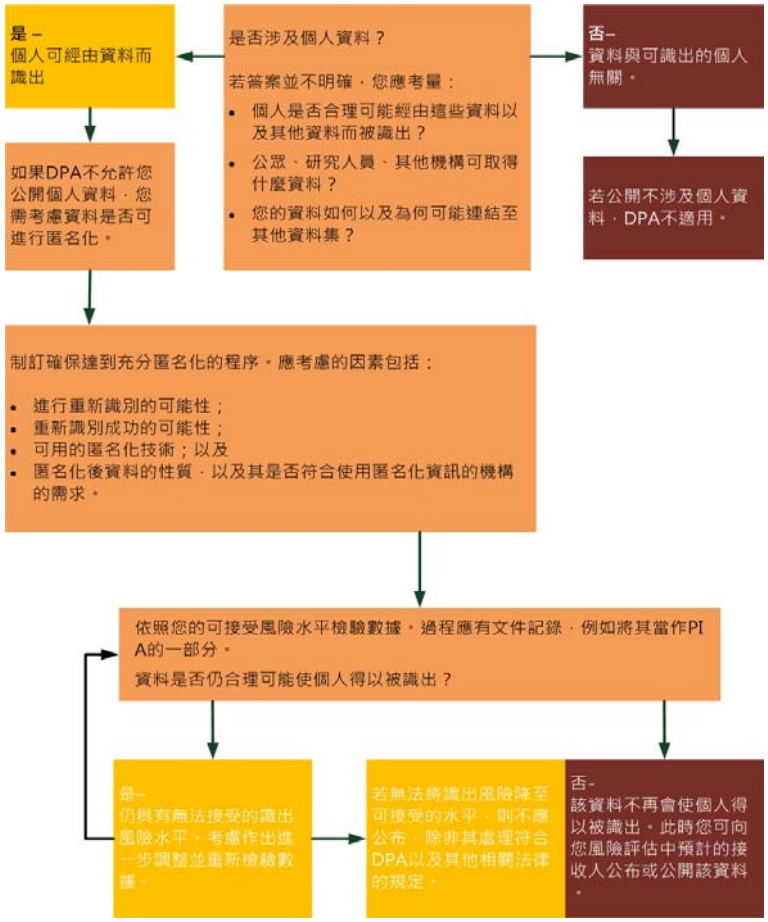

圖 5、個人資料開放流程

資料來源：英國去識別化作業規範

2. 確定去識別化有效性

依據資料保護法規定，個人資料代表與現存個人之關聯，該個人可經由此等資料，以及資料控制者目前或將來可能擁有的資料而識別之。可能為某些組織、某些公眾成員、或所有民眾皆可取得的其他資訊，例如：網路公開資訊，於聯結去識別化後的資料後，始得重新識別的風險難以預測，因為無法斷言哪些資料是可取得或哪些資料可能會在未來公開。資料一旦公開，因確保其刪除或移除有所困難或難以實現，資料往往無法重新獲得保障（即撤回資料或由網站中移除）。因此於產生與公開去識別化資料的初始階段，須盡可能地執行風險分析。

(1) 重新識別

重新識別有兩種主要方式：

- 入侵者依所擁有的個人資料搜尋經去識別化資料集進行匹配。
- 入侵者依去識別化資料集的記錄，搜尋公開資訊進行匹配。

公開個人資料的風險與公眾利益，並非資料保護法所允許在判定資訊是否為個人資料時的考量因素。但在實務上，某些類型的資料對蓄意入侵者將更具吸引力，並對當事人影響更大。根據資料的性質、內容，以及關乎何者，識別出當事人可能產生各種不同後果。

資訊專員公署認為實際運作時，肯定會有難以判斷是否會被重新識別的情況。若被重新識別而使當事人遭受痛苦、蒙受損害或經濟損失，組織可採取以下作法：

- 尋求個人資料當事人同意資料公開，說明可能的後果；
- 採用更嚴格的風險分析與去識別化方法。

資料控制者需了解重新識別的風險，以及此種風險可能隨著時間而改變，審慎評估未來重新識別風險的發生可能性。依據目前與未來可能的威脅，定期檢視其公開資料的政策與去識別化技術。

(2) 定性資料去識別化

許多被創建、使用與公開的經去識別化資料是出自政府之資料集，本質上係統計資料。但是，當試圖將定性資料去識別化時，用於去識別化定性資料的技術並非普遍適用，例如：會議記錄、採訪記錄或影片，需使用不同的技術。常用的方法包括：

- 在文件中除去個人姓名；
- 模糊影片以掩藏面孔；
- 電子掩藏或重新錄製聲音資料；
- 改變報告細節（確實的地名、日期等）。

定性資料之去識別化往往十分費時。不利於大量處理，可能需要人工

根據該資料進行判斷。

(3) 「蓄意入侵者」檢驗

「蓄意入侵者」係不具備任何事前知識的人士，希望藉由所取得的個人資料以及去識別化資料而識別出當事人。該方法假定「蓄意入侵者」可取得如網路、圖書館，以及公開文件等資源，且會採用調查技術，如詢問可能擁有個人資料當事人其他資訊的人士，或逕行宣傳使知悉資訊的人士主動提供。同時假定「蓄意入侵者」不具備任何的專業知識（如電腦駭客技術）、或能使用專業設備或不從事犯罪行為（如盜竊）所取得的安全保護的資料。實務上進行蓄意入侵者檢驗可能包括：

- 進行網路搜尋，了解結合出生日期以及郵遞區號資料能否識別特定個人的身分;
- 搜索國家或地方報紙檔案，了解是否有可能把受害者的名字連結到犯罪地圖資料；
- 使用社群網路，了解匿名資料是否會連結到使用者個人資料；
- 使用選民名冊與地方圖書館資源，嘗試連結匿名資料與某人身分。

藉由蓄意入侵定期重新評估重新識別的風險是很好的作法，當電腦技術演進與資料公開程度增加時，重新識別的風險亦增加，若造成個人資料被重新識別，處理的組織將承擔自身的資料保護責任。

3. 個人資料與空間資訊

依據資料保護法處理空間資訊並無一定規則（如郵遞區號、GPS 資料或地圖索引）。於某些情況下，其將被視為個人資料，例如：關於某個寓所或房產的資訊。相關資訊的脈絡以及其他變數十分重要，諸如特定郵遞區號所覆蓋的家庭數量，越完整的郵遞區號（或更精準的地理片段資訊）越能進行分析，或與其他資訊結合，從而造成個人資料公開。空間資訊一般會與持有的資料集規模有關，須視個案考量其地點。

(1) 郵遞區號

將郵遞區號去識別化，一般會採取除去或模糊某些位數，減少被識別出的風險。在去識別化的過程應考量郵遞區號的特性，例如：全碼郵遞區號所代表的戶數、去尾數郵遞區號代表的戶數、各郵區的戶數等因素。替換郵遞區號亦是一種替代方案，雖可保留資料的詳盡度與準確性，但不適合公開資料。

(2) 智慧型手機與GPS

行動裝置,例如:智慧型手機與 GPS 系統能產生大量的詳細空間資訊。該空間資訊是否能識別個人與相關資訊，取決系統如何運作。組織應考量其他的獨特標識符（如 IP 位址）以及其他身分資訊（如姓名、地址）如何

連結到空間資訊。智慧型手機用戶通常會選擇是否讓其裝置或特定 APP 揭露其位置。對個人而言，裝置或 APP 如何使用該資訊應要十分明確。隱私政策應明確規定空間資訊是否被當作個人資料來處理，以及何時須去識別化。

「降級」或「弱化」的個人資料，此概念對使用空間資訊的組織而言十分受用。組織為使業務得以進行會需要將空間資訊當作個人資料處理，在目的達成後，便不需要準確的空間資訊。其後，詳細資訊可以逐漸代換為更為廣泛的資訊。例如，有關使用者精確 GPS 坐標的資訊可代換為街道名、區名、然後僅有城市名。位置資訊可藉由以下方式降低隱私風險：

- 加大製圖區域，以覆蓋更多房地產與居民；
- 減少公布的頻率與及時度，使其得以涵蓋更多事件，難以識別近期案例，或不揭露其他資料，例如事件的時間或日期；
- 在移除 IP 位址的末 8 位元，以降低所含有的地點資訊；
- 使用格式，如熱圖，其提供一個全貌，而不顯示特定地點或人士的詳細資訊；
- 避免公開住家等級的空間資訊，因為可輕易地連結某一處房產或居民（例如：使用可公開獲得的選民名冊）。

4. 公開形式

去識別化資料使用者會希望資料豐富可用，能符合其用途，但亦不希望發生被重新識別。事實上，不同類型的去識別化資料存在不同程度被重新識別的弱點。例如，使用化名所保留的個人特性較高亦可以透過不同來源的化名紀錄比對，意謂著較高的重新識別風險；而總體資料相對的風險可能較低，取決於明晰度、樣本規模等等，然而，總體資料可能不具有資料聯結或個人層級分析所需的細節度，而此係資料研究分析所仰賴的。

去識別化資料控制者須審慎地考量公開選項（即資料是否需要公布或限制存取是否較合適？），一般而言，去識別化資料越詳盡、越可連結、越接近個人層級，其存取的限度就應該更嚴謹，而去識別化資料越是一般、越不可連結，越得以公布。

(1) 公開與限制存取

充分公開去識別化資料與限制存取應有所區別，開放資料固然可提高大眾可用性，但依據 2000 年資訊自由法，公開資料不可侷限於特定個人或群體。然而，許多研究、系統規劃與測試，藉由將資料在封閉社群內公開的方式進行（即僅有有限數量的研究人員或組織得以取用資料，且不得進一步公開，如經由契約）。如此做的好處是，重新識別以及其他風險更加可

控制。

處理敏感性去識別化資料或重新識別風險較高時,限制存取尤其適合。限制存取公開仍可能具有相關風險，此時，可以徵求用戶同意，有限地公開記錄層級資料。

(2) 限制存取保護

首次限制存取公開的組織，在其他人士取用資料前，須建立相關保護措施，包括：

- 用途限制，即接收人只可將資料用於既定的用途（或既定一系列用途）；
- 資料取用人員需接受資料保護與資料最小化之教育訓練；
- 資料取用人員的背景調查；
- 控制將其他資料帶進該環境中的能力，管理因連結或關聯而產生的重新識別風險；
- 將資料的使用限於特定計畫或系列計畫；
- 限制資料的公開；
- 禁止任何重新識別的意圖以及未預期重新識別個人資料的銷毀措施；
- 組織安全措施，如員工保密協議；
- 加密以與金鑰管理，以限制資料的取用；
- 限制資料的影印，或影本數目；

- 計畫結束後安排資料銷毀與歸還；
- 懲處，如違反其條件時可能施加於接收人契約懲處。

資料控制者須定期進行風險評鑑，例如使用組織的日常資料安全風險評估程序，參與計畫的組織間彼此合作謀求安全性措施。

5. 管理

資料去識別化與公開須在有效的管理架構下進行，若主管機關收到資料處理投訴（包括去識別化）或進行稽核時，管理架構能提供有效協助，透過管理架構證明遵循法令規範，且有正當理由相信所公布的資料中不含個人資料或具有重新識別風險。

(1) 管理架構

管理架構應涵蓋以下幾個方面。

- 負責授權與監督去識別化處理，應為俱備足夠資歷，對技術與法律知識、能管理處理的人士，例如：「資深資訊風險負責人」（Senior Information Risk Owner, SIRO）。SIRO 須承擔關鍵決定的責任，協助決定去識別化的通則，並決定合適的公開形式（即公布或限制存取）。
- 員工訓練：員工應清楚理解去識別化技術、所涉及的風險以及減輕風險的方法，以及去識別化作業中所扮演的角色。
- 當去識別化作業有所疑慮或難以執行時：可能為難以評估重新識別

的風險，或可能對個人造成極大的風險，應記錄相關決策，包括是否去識別化的決定、如何進行、是否公開。

- 定期更新去識別化相關的法規、指引或判例等資訊，同時亦包括去識別化的新技術與入侵者在資料集中識出個人的新技術。
- 與相關產業的其他組織或進行類似工作的組織合作，共同組織分享公開的相關資訊，以評估被識別的風險。
- 隱私衝擊評鑑（Privacy Impact Assessment, PIA）：為評估隱私風險的有效結構性方法，隱私衝擊評鑑可能包含去識別化技術有效性測試，以評估重新識別風險與制訂控制措施。
- 透明度：當去識別化資料對所有個人都沒有直接影響時，可能沒有通知個人資料當事人的必要性。但隱私權政策應清楚地說明去識別化措施與後果，包括：
  - ✓ 說明為什麼要進行去識別化與使用的去識別化技術；
  - ✓ 說明是否個人擁有其個人資料去識別化的選擇權，若有，該如何行使與相關聯絡細節；
  - ✓ 說明減輕去識別化資料相關風險的保障措施；
  - ✓ 說明匿名資料是否會公開或是有限揭露；
  - ✓ 說明去識別化的相關風險，以及可能產生的後果；
  - ✓ 公開說明公開去識別化資料的論據程序，解釋如何「權衡」、考量哪些因素、為何如此考量以及如何「無死角」地觀察被識別，提升個人資料當事人的信任度；
  - ✓ 組織亦應考量公布去識別化 PIA 報告，並在需要時刪除某些資訊或僅公布概要報告。
- 檢視去識別化的結果，特別是分析回饋意見。檢視為持續進行的活

動，應使用「重新識別檢驗」技術評估重新識別風險，並降低其風險，分析並且處理投訴與詢問（來自認為隱私受到侵犯的大眾）。

- 災害應變：若重新識別確實發生並且個人隱私洩露時的應變措施，包含告知個人資料當事人，協助他們採取必要的救助措施。重新識別事件可能導致去識別化程序中止或修訂去識別化程序（例如使用更嚴格的去識別化技術或公開控管）。

(2) 重新識別檢驗

重新識別檢驗（一種「滲透」檢驗）能檢測重新識別漏洞，應嘗試利用一個或多個匿名資料集以重新識別個人。經由第三方組織進行檢驗通常較容易找到忽略或未知資料來源、技術或漏洞類型。

重新識別檢驗程序的第一階段應盤點組織已公布或欲發布的匿名資料，第二階段應嘗試可取得哪些其他資料（無論是否為個人資料），能連結到去識別化資料。實務上可能難以或無法確定特定個人或組織能取得的資訊，但是還是得詳實地確認是否有其他可取得的公開資料（或透過網路搜尋取得），可能導致重新識別。前文所述「蓄意入侵者」檢驗可為滲透檢驗有用的要素。貫穿檢驗應符合以下標準：

- 應嘗試識出特定個人與一或多項與個人有關的特徵；
- 採取所有入侵者合理可能使用的方法；
- 使用任何合法獲得、可能用來識別資料集中特定個人的資料來源。

當涉及統計資料時，重新識別風險評估變得更加複雜，因為有可能可公開取得之各種統計資料集，在使用特定方式匹配時，有可能導致重新識別。亦可能有使用某特定資料集本身的資料而產生的重新識別風險。

四、 國際標準組織

(一) OECD 隱私指導原則

由歐美國家組成的經濟合作與發展組織（Organization for Economic Co-operation and Development, OECD），於 1980 年公布（並於 2013 年改版）保護隱私與跨境傳輸個人資料的隱私指導原則（Guidelines on the Protection of Privacy and Transborder Flows of Personal Data），成為世界各國廣泛認可的隱私保護實務參考，同時亦受美國聯邦貿易委員會（FTC）支持。其中提出 8 項隱私保護原則，適合組織作為制定隱私保護政策時的參考。

1. 限制蒐集原則（Collection Limitation Principle）

個人資料蒐集應受限，且要以合法及公平方式取得，同時以適當方式取得當事人同意及知悉。

2. 資料品質原則（Data Quality Principle）

個人資料內容應與蒐集目的相關，或是符合其利用目的而產生的必要性，

必須確保個人資料內容之正確性與完整性，並及時更新。

3. 目的明確原則（Purpose Specification Principle）

個人資料之蒐集目的，必須在開始蒐集時即明確指出，隨後在利用此等個人資料時，必須限制於初始目的內，後續若需變更，要明確指出其變更後之利用目的為何。

4. 利用限制原則（Use Limitation Principle）

除非已事先獲得當事人同意或依據相關法律，個人資料不應有特定目的外之揭露或利用。

5. 安全保護原則（Security Safeguards Principle）

針對個人資料可能發生遺失、不當存取、利用、修改、損毀及揭露之風險，應採取適當的安全控制措施，以降低可能風險。

6. 公開原則（Openness Principle）

對於個人資料的發展、實務和政策的制定，應依據公開的原則進行，針對個人資料持有的種類及使用目的，以及資料控制者的連絡方式，應公開且易於讓當事人知悉。

7. 個人參與原則（Individual Participation Principle）

個人資料當事人，應具有以下權利：

- 有權向資料控制者或持有之組織，確認是否持有與其相關的個人資料；
- 向組織查詢與其有關之個人資料，於合理時間內及合理收費下，組織須以合理的方式及可了解的形式提供之；
- 針對所提出的查詢或主張的權利若遭到拒絕時，可提出異議要求說明；
- 若所提出的異議成立時，可要求組織刪除、變更、修改、補充其個人資料。

8. 歸責原則（Accountability Principle）

個人資料控制者須負起相關責任，並落實以上各項隱私保護原則。

(二) APEC 的隱私保護框架

亞太經濟合作組織（APEC）針對隱私維護與個人資料保護的要求，在 2003 年成立資料隱私保護小組（Data Privacy Subgroup），並於 2004 年通過隱私保護框架（APEC Privacy Framework），包含以下 9 項隱私保護原則：

1. 損害避免（Preventing Harm）原則

體認當事人對其個人資料的合理期待，對可能損及當事人權益的風險，應採取適當的風險處理措施以避免損害。

2. 告知（Notice）原則

於蒐集個人資料時，應告知當事人蒐集目的、資料型式、蒐集者之聯絡方式與當事人可主張權利。

3. 限制蒐集（Collection Limitation）原則

個人資料之蒐集應與告知的目的相關，要求採取公正的方式進行，並限制所蒐集的範圍。

4. 利用（Uses）原則

個人資料之利用應獲當事人同意，且僅限於蒐集之最初目的範圍內，不可作為目的外用途。

5. 選擇（Choice）原則

應提供予當事人選擇之權利，能針對其個人資料的蒐集、處理及揭露，主張其個人的意願選擇。

6. 完整性（Integrity）原則

應確保個人資料之正確性與完整性，並持續更新，以維護當事人權益。

7. 安全保護（Security Safeguard）原則

持有個人資料的組織，應對可能的安全風險，實作對應的控制措施，以避免個人資料受不當的揭露與損毀。

8. 存取及更正（Access and Correction）原則

組織應提供個人資料當事人，於合理時間內，以適當方式提出請求，查詢其個人資料，且不得無故拒絕補充或更正個人資料的請求。

9. 歸責（Accountability）原則

個人資料控制者應對遵守上述原則的措施負責。當個人資料無論是在國內還是國際被傳輸至他方，個人資料控制者應獲得當事人同意或是進行盡責調查，並採取合理步驟確保資料接受者將遵循此等原則保護資料。

(三) 雲端安全聯盟

2016 年，雲端安全聯盟（Cloud Security Alliance, CSA）發佈巨量資料安全與隱私手冊，提供了巨量資料安全與隱私的 100 項實作建議，其中也

涵蓋了去識別化機制之實作建議：

1. 去識別化資料

應確保資料當事人身分是否會與外部資料連結，若存在連結則可能損及資料當事人隱私,所有個人可識別資訊(Personally Identifiable Information, PII)，例如姓名、地址、身分證字號等都必須遮蔽或移除。此外對於準識別符，包括足以唯一識別資料當事人的數據，例如郵遞區號、出生日期、性別，都應採用 K 匿名等去識別化技術，減少重新識別的風險。

2. 重新識別技術

重新識別通常係指去識別化個人資料與資料當事人匹配的過程，為保護消費者隱私權益，個人可識別資訊，如姓名與身分證字號通常會被包含敏感資訊的資料庫中移除。

- 使用匿名或去識別化資料保護消費者隱私，亦可以提供行銷或資料採礦公司進行分析。
- 建立隱私標準，以防堵重新識別的機會。

(四) 歐洲網路與資訊安全局

2015 年，歐洲網路與資訊安全局（European Network and Information

Security Agency, ENISA）公布巨量資料隱私設計報告，該報告說明巨量資料分析時的隱私強化技術，並提及在巨量資料時代，去識別化要兼顧資料集合實用性有其難度，且會隨著資料量與種類而增加，使用較低強度的去識別化技術，例如抑制直接識別符，通常無法確保不可識別性，但若使用高強度的去識別化技術，又將阻礙不同來源的同一個人（或類似個人）的數據連結，降低巨量資料分析的效益。該報告並提出以下觀點：

- 受控制的可連結性：

防止連結紀錄是去識別化的普遍目標，就巨量資料而言，除滿足防止重新識別與屬性揭露外，最好也能允許存在部分可連結性。實際操作上，巨量資料去識別化應該兼容部分（去識別化）來源的資料連結。

- 動態與串流資料的去識別化：

巨量資料中存在許多連續性的資料流量（例如傳感器的數值），因此需關注資料流量的揭露風險控制。

- 巨量資料的可運算性：

巨量資料中，即使只是靜態資料集合，其資料量也可能非常龐大，而形成去識別化的挑戰，在選擇隱私模型與去識別化技術時，須考量運算效率。

第二節 我國通訊傳播事業個人資料保護機制

目前歐盟具有全世界最先進之個人資料保護架構，我國於 1995 年 7 月完成立法施行之「電腦處理個人資料保護法」及 2010 年 5 月修正通過之「個人資料保護法」，其中許多條文係參考歐盟 1995 年之資料保護指令（95/46/EC）。在歐盟規範架構下，政府資訊涉及個人資料時，其開放公眾利用仍須受個人資料保護指令之限制。

然隨著資訊科技及網際網路高速發展，以及行動裝置之大量使用，始得人們可隨時隨地大量且快速蒐集網路上之各種個人資料，再自動進行巨量資料分析，得以了解個人消費傾向，用以尋求新商機。然此常係於當事人未知下，利用個人資料於非預期目的。而因數位化資料留存於電腦網路，具無時間、空間限制之特性，經常涉及個人資料事件發生許久後，個人資料仍存在於網路上。因當事人對個人之資料存於網路上何處、由何人持有及被如何利用難以掌握，難以主張個人資料之隱私權。因應現今新形式之個人資料蒐集、處理及利用，當事人隱私權處於被侵害之高風險下，有必要規範通訊傳播事業於利用資料進行巨量資料分析及公開資料前，將個人資料去識別化的相關程序與規定。

一、　個人資料保護法

(一) 個人資料定義

依個人資料保護法第 2 條第 1 款規定，個人資料是指姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。直接識別之個人資料指接觸該資料之人，可直接將該資料與特定人連結，一般而言「姓名」被認為屬直接識別之個人資料，然姓名須限於足以特定之範圍，例如班級、辦公場所等。但並不以此為限，只要於具體情形得以直接透過該資料與特定個人建立連結，從而自群體中識別出該特定個人者均屬之，例如國民身分證統一編號、護照號碼、學校學號等。

所謂「得以間接方式識別」依個人資料保護法施行細則第 3 條規定，係指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。又所謂經由對照、組合、連結等方式識別特定個人，必須是精準且確定地得以識別出特定個人，而非僅是利用專業知識「猜測」、「推測」可能為某人之資料，即使該「猜測」或「推測」結果是正確的，亦不能因而認為猜測者有取得該個人資料。

(二) 個人資料保護

個人資料保護法施行細則第十二條：為防止個人資料被竊取、竄改、毀損、滅失或洩漏，組織應採取技術上及組織上之措施，並以與所欲達成之個人資料保護目的間，具有適當比例為原則。此等措施至少包括下列事項：

- 配置管理之人員及相當資源；
- 界定個人資料之範圍；
- 個人資料之風險評估及管理機制；
- 事故之預防、通報及應變機制；
- 個人資料蒐集、處理及利用之內部管理程序；
- 資料安全管理及人員管理；
- 認知宣導及教育訓練；
- 設備安全管理；
- 資料安全稽核機制；
- 使用紀錄、軌跡資料及證據保存；
- 個人資料安全維護之整體持續改善。

(三) 個人資料判斷之相對性

個人資料保護法施行細則第 3 條：所稱「得以間接方式識別」，指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、

組合、連結等，始能識別該特定之個人。

因得為比對組合之人及資料範圍具有「相對性」，故難有一致性、明確性之認定標準，欲判斷一份資料是否為個人資料，對於不同蒐集者而言，即可能會產生不同之判斷結果（個人資料保護法施行細則第 3 條修正理由參照）。

(四) 去識別化之行為定性

個人資料去識別化之行為應定性為個人資料保護法第 2 條第 4 款所稱之「處理」，而我國個人資料保護法之體系架構係將「蒐集」及「處理」行為規範於相同法定要件之下，蓋個人資料之「蒐集」大多緊密伴隨著「處理」行為，故個人資料保護法並未特別區隔兩者之行為要件，且因去識別化資料須達到無從直接或間接識別特定人之程度，故去識別化之加工處理並未增加對當事人權益之額外侵害，因此，如原先蒐集個人資料之行為符合個人資料保護法第 15 條及第 19 條第 1 項之規定，應可認為去識別化之處理並未逾越原先蒐集之特定目的，而得依據原先蒐集時之同一合法事由為之。

(五) 個人資料保護與去識化之適法性分析

法務部民國 103 年 11 月 17 日法律字第 10303513040 號函指出：「如將公務機關保有之個人資料，運用各種技術予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者，即非屬個人資料，自非個人資料保護法之適用範圍。」

法務部上開函釋與德國、英國資訊保護官及英國法院見解相同，固然公務機關仍然保有原始資料或對照表等工具得以直接或間接識別相關當事人，故公務機關所保有的整體資料仍然屬於個人資料，但其對外主動公開或被動提供去識別化後之資料並無違反個人資料保護法的問題，因為當該資料對外公布釋出之時，其已不再是個人資料。

(六) 以風險影響評估及控制為去識別化基礎

公務機關應評估個人資料隱私的整體風險影響，綜合考量個人資料類型、敏感性程度、對外提供資料之方式、引發他人重新識別之意圖等因素，並根據風險評估之結果計算設定風險檻值，進而判斷去識別化之技術類型或程度。

1. 開放資料（Open Data）

因並未限制資料提供之對象、使用目的或方法，而是以公開之方式提供，因此風險檻值相對較高，宜達「去識別化資料」或「不可逆之擬去識別化資料」之程度較為妥適。

2. 限制存取（limited access）

因資料提供對象有所限縮除能對於資料接收者之身分、使用目的、其他可能取得資料之管道、安全管理措施等先為必要之審查外，並得與資料使用者約定禁止重新識別資料之義務及其他資料利用之限制等，較有利於風險的控管，因此風險檻值相對較低，去識別化之程度可相對放寬，可提供含有個體性、敏感性、較為詳細之擬去識別化資料。

(七) 加工匿名後無從識別之判斷標準

採一般人基準說（同英國見解），有先前知識（prior knowledge）之人，對於當事人所增加之隱私風險實際上很低，因其原本就已經保有當事人原始的個人資料才有能力得以重新間接識別，所以重點應不在此群人得否識別當事人，而在於其能否透過釋出之資料而取得當事人的新個人資料。

多數具有先前知識之醫師、律師等專業人員，雖掌握大量敏感性個人

資料（病歷、犯罪前科等），但多已依法令負有保密義務或須遵守職業倫理規範。

二、　電子通訊傳播法草案

(一) 背景

鑒於科技匯流業已逐漸弭除傳統通訊傳播產業間壁壘分明之界線，跨媒體之經營亦影響新世代通訊傳播技術及服務發展模式，曩昔依業別不同，而循個別管制政策目的分別立法規管之垂直管制模式，實有重新檢視正當性而進行調整之必要。

有別於傳統通信或媒體，在網路 WEB 2.0 概念下，網際網路參與者之身分趨於流動化，使用人亦可能同時具備提供電子通訊傳播服務者之角色，非為固定、單向，更跨越國境藩籬。傳統分流之電信、廣播電視及電腦網路已藉由網際網路高度匯流，現今之使用人與提供電子通訊傳播服務者實係居於對等之地位，故本法以電子通訊傳播為規範主體，民事權利義務關係為主軸，揭櫫電子通訊傳播行為之一般性規範。[51]

[51]電子通訊傳播法草案，105 年 5 月，總說明。

(二) 隱私權與資訊政策

第 12 條提供電子通訊傳播服務者應依其服務之性質，以得清楚辨識之方式公告其服務使用條款；個人資料保護條款如下：

1. 隱私權及資訊政策：

- 適用之範圍及例外；
- 蒐集之資訊類型及目的；
- 使用資訊之方式；
- 提供使用人存取、使用及更新資訊之服務方式。

2. 資訊安全政策，包括惡意程式之避免及帳戶資料之安全。

三、 去識別化機制

(一) 個人資料去識別化定義及型式

所謂「個人資料去識別化」，即指透過一定程序的加工處理，使個人資料不再具有直接或間接識別性。依其去識別化之加工程度不同，有以下「匿名化資料」及「擬匿名化資料」之類型：

- 匿名化資料（anonymised data）：對任何人而言，均無法採取任何合理可能之方法識別特定個人，亦即資料經加工後，毫無保留連結之可能性。
- 擬匿名化資料（pseudonymised data）：擬匿名化資料乃是以編碼或

別名取代識別符（例如姓名、國民身分證統一編號等），使研究或統計人員得以針對個體資訊進行分析而無須識別個體身分，可再細分為 2 種型式：

- ✓ 不可逆（non-retraceable/irreversible）：由經去識別化之資料無法回復原始資料。
- ✓ 可逆（retraceable/reversible）：由經去識別化之資料可回復原始資料。多用於特定依法允許重新識別之領域，例如：醫療實驗研究時，能回溯追蹤調整對受試病患之醫療處置。

若個人資料已「去識別化」達到無從識別個人資料當事人，而為「匿名（anonymous）」之狀態，歐盟認為此時已非個人資料，自無歐盟個人資料保護指令之適用，原則上應屬政府資訊開放公眾利用之範圍，惟去識別化的資料必須達到「以一切可能合理之方法（all the means likely reasonably to be used）」無從再識別個人資料當事人之程度，否則仍應受個人資料保護指令規範。法務部認為我國採取相同論點。

如何界定「個人資料已去識別化」，在巨量資料時代有其困難性及不確定性，即使依當時科技或專業水準被認為已去識別化的資料，日後隨著資料的不斷累積、資訊技術的發展演進、資料儲存成本的下降，仍可能透過與其他資料的對照、組合、連結而被重新識別。

(二) CNS29100 標準

CNS 29100（資訊技術－安全技術－隱私權框架）標準提供資通訊技術（Information and Communication Technology, ICT）系統內保護個人可識別資訊（Personally Identifiable Information, PII）之高階框架。本質上其係通用的，並將組織、技術及程序各層面置於整體隱私權框架中。

此隱私權框架欲協助組織於 ICT 環境中，藉由下列項目定義其與 PII 有關隱私保全之要求事項。

- 規定共同之隱私權專門用語；
- 定義處理 PII 之行為者及其角色；
- 描述隱私保全要求事項；
- 提供已知隱私權原則之指引。

1. 規定 PII 流向及其角色

就 PII 當事人、PII 控制者及 PII 處理者間可能之 PII 流向而言，可識別下列情境。

（a）PII 當事人提供 PII 予 PII 控制者（例：於註冊 PII 控制者所提供之服務時）。

（b）PII 控制者提供 PII 予 PII 處理者，其代表 PII 控制者處理該 PII（例：作為委外協議之一部分）。

（c）PII 當事人提供 PII 予 PII 處理者，其代表 PII 控制者處理該 PII。

（d）PII 控制者提供與該 PII 當事人有關之 PII 予 PII 當事人（例：依 PII 當事人之請求）。

（e）PII 處理者提供 PII 予 PII 當事人（例：依 PII 控制者指示）。

（f）PII 處理者提供 PII 予 PII 控制者（例：於履行所約定服務後）。

（g）上述情境中 PII 當事人、PII 控制者、PII 處理者及第三方角色於表 4 說明。需區分 PII 處理者與第三方，係因 PII 送交 PII 處理者時，其法定控制仍屬原 PII 控制者，而第三方一旦接收該 PII 即可獨立成為 PII 控制者。例如，當第三方決定接收自 PII 控制者之 PII 傳送至他者時，其將獨立扮演 PII 控制者，因而不再被視為第三方。就 PII 可能流向，一邊為 PII 控制者及 PII 處理者，與另一邊為第三方，可識別下列情境。

（h）PII 控制者提供 PII 予第三方（例：依商業協議或 PII 控制者指示）。

上述情境中 PII 控制者與第三方之角色亦於表 4 說明。

表 4、PII 流向與角色

	PII 當事人	**PII 控制者**	**PII 處理者**	**第三方**
情境（a）	PII 提供者	PII 接收者	—	—
情境（b）	—	PII 提供者	PII 接收者	—
情境（c）	PII 提供者	—	PII 接收者	—
情境（d）	PII 接收者	PII 提供者	—	—
情境（e）	PII 接收者	—	PII 提供者	—
情境（f）	—	PII 接收者	PII 提供者	—
情境（g）	—	PII 提供者	—	PII 接收者
情境（h）	—	—	PII 提供者	PII 接收者

資料來源：CNS 29100

2. CNS 29100 隱私權原則

A. 同意及選擇

- 向 PII 當事人表明，以選擇是否允許處理其 PII，除非 PII 當事人無不同意之自由，或所適用法律允許無須該自然人同意即可處理 PII。PII 當事人之選擇必須是自由提供、特定且基於充分理解；
- 取得 PII 當事人選擇加入之同意以蒐集或其他方法處理敏感 PII，除非適用之法律允許無須該自然人同意下處理敏感之 PII；
- 於取得同意前，通知 PII 當事人關於其在個人參與及存取原則下之權利；
- 於取得同意前，向 PII 當事人提供以公開、透明及告知原則所表明之資訊；
- 向 PII 當事人解釋給予或不予同意之涵義。

B. 目的適法性及規定

- 確保（各）目的均遵從適用之法律且依賴所允許的法律基礎；
- 在為新目的而蒐集或第一次使用資訊之前，向 PII 當事人傳達（各）目的；
- 該規定宜使用清楚且適合環境之用語；
- 若適用，充足解釋處理敏感 PII 之需要。

C. 蒐集限制

- 將 PII 之蒐集限制於適用之法律及嚴格地為此指定目的所必要之邊界範圍內；
- 組織不宜任意蒐集 PII。蒐集之 PII 數量及型式二者均宜限制於符合由 PII 控制者規定之（合法）目的所必須者。組織於進行蒐集 PII 之

前宜審慎考量哪些 PII 係為實現特定目的所需。組織宜文件化所蒐集 PII 之型式及其理由，納入其資訊處理政策及實務；

D. 資料極小化

- 將所處理之 PII、隱私權利害相關者及 PII 揭露對象或可存取 PII 之人員的數目最小化；
- 確保採用〝僅知（need-to-know）〞原則，亦即於 PII 處理之合法目的框架下，宜僅對執行正式職務所必要之人員賦予 PII 存取權限；
- 使用或提供預設選項，只要不涉及 PII 當事人之識別的互動及交易，儘可能降低其行為之可觀察性並限制所蒐集 PII 的可連結性；
- 一旦 PII 處理之目的終止，無法定要求保有 PII，或是實務上需如此做時，即刪除或廢棄 PII。

E. 利用、持有及揭露限制

- PII 之利用、持有及揭露（包括移轉）限制於為履行特定、明確及合法目的所必要者；
- 除非適用之法律明確要求不同的目的，否則將 PII 之利用限制於蒐集之前 PII 控制者所規定之目的；
- 持有 PII 之時間長度，僅為滿足所陳述目的必要的長度，並於之後安全地將其破壞或去識別化；
- 一旦所陳述目的逾期，但依適用法律要求保留下，鎖住（亦即將 PII 歸檔、保全及免除進一步處理）所有 PII。

F. 準確性及品質

- 確保所處理之 PII 準確、完整、最新（除非有保有過期資料之合法依據）、適度的，且與使用目的相關；

- 於處理前，確保由非 PII 當事人之來源所蒐集的 PII 之可靠性；
- 變更 PII 前，經由適當方法查證 PII 當事人聲明之有效性及正確性（以確保該等變更經適當授權）；
- 建立 PII 蒐集程序，以協助確保 PII 之準確性及品質；
- 建立控制機制，以定期核對所蒐集及儲存之 PII 的準確性及品質。

G. 公開、透明及告知

- 提供予 PII 當事人，關於 PII 控制者對於處理 PII 之政策、程序及實務的清楚且易取得之資訊；
- 告知中包括，處理中之 PII、處理目的、PII 可能揭露對象之隱私權利害相關者型式，以及 PII 控制者身分含 PII 控制者之聯絡資訊；
- 揭露 PII 制者提供予 PII 當事人之選擇及方式，以限制處理、存取、修正及移除其資訊；
- 當 PII 處理程序發生重大變更時，告知 PII 當事人。

H. 個人參與及存取

- 給予 PII 當事人存取及審查其 PII 之能力，只要其身分先經適當保證等級鑑別，且該存取未被適用之法律禁止；
- 允許 PII 當事人質疑 PII 之準確性及完整性， 並在特定全景內， 於適當及可能時修訂、更正或移除；
- 於知悉對方之情況下，對 PII 處理者及個人資料揭露對象之第三方提供所有修訂、更正或移除資訊；
- 建立程序，使 PII 當事人得以簡單、快速及有效率之方式行使其權利，且不造成不應有之延誤或成本。

I. 可歸責性

- 於適當時，記錄及溝通所有隱私相關政策、程序及實務；
- 於組織內指派所規定之個人（於適當時可能依序委派組織內其他人），實作隱私相關政策、程序及實務之任務；
- 當傳送 PII 至第三方時，確保第三方接收者一定會經由契約或其他如強制之內部政策（適用之法律可包含關於國際資料傳輸之額外要求）等手段，提供相同等級之隱私保護；
- 為可存取 PII 之 PII 控制者提供合適的訓練；
- 設立有效率之內部抱怨處理及糾正程序供 PII 當事人使用。
- 通知 PII 當事人關於可能對其造成實質損害之隱私權違反（除非被禁止，例：當與執法人員一起工作時），以及採取之解決方法；
- 於某些管轄權（例：資料保護主管機關）中之要求及依據風險等級，通知所有相關之隱私權利害相關者，隱私權違反事件；
- 若發生隱私洩露，允許受侵害之 PII 當事人，存取適當及有效的制裁及/或補救，如矯正、消除或賠償；
- 就自然人之隱私狀態難以或無法回復至事前狀態，考量其補償程序。

J. 資訊安全

- 於主管機關許可下，於運作、功能及策略層級上以適宜之控制措施保護 PII，以確保 PII 之完整性、機密性及可用性， 並於其整個生命週期中保護其免受未經授權之存取、破壞、使用、修改、揭露或損失的風險；
- 選擇 PII 處理者，其對 PII 處理之關於組織、實體及技術的控制措施

提供充分保證，並確保遵循此等控制措施；

- 依據適用之法律要求、安全標準、CNS 31000 中所描述之系統化安全風險評鑑的結果，以及本益分析之結果，建立此等控制措施；
- 實作控制措施，相稱於潛在後果之可能性及嚴重性、PII 之敏感性、可能受影響之 PII 當事人數目，以及其被持有之全景；
- 對要求存取權限以執行其職責之個人，予以 PII 存取限制。限制上述個人之存取， 僅限於其執行職責所需存取之 PII；
- 解決經由隱私風險評鑑及稽核過程，所發現之風險及脆弱性；
- 於持續之安全風險管理過程中，須定期審查及重新評鑑以管制控制措施。

K. 隱私遵循

- 藉使用內部稽核員或受信賴第三方稽核員，定期實施稽核以查證及證明處理符合資料保護及隱私保全要求事項；
- 擁有合適之內部控制措施及存在獨立之監督機制，以確保遵循相關隱私權法律及其安全、資料保護及隱私權政策與程序；
- 發展及維護隱私風險評鑑，以評估涉及 PII 處理之方案及服務遞送組織是否遵循資料保護及隱私要求事項。

(三) CNS29191 標準

CNS 29191（資訊技術－安全技術－部分匿名及部分去連結鑑別之要求事項）標準規定部分匿名及部分去連結鑑別之框架及其要求事項。

目前先進之個體鑑別技術，要求揭露待鑑別個體的可識別資訊。於諸

多形式之交易中，傾向於將個體保持匿名及去連結，意即當履行 2 個交易時，難以區別該等交易係由同一使用者或由不同使用者所履行。然而，於某些具正當理由之情況下，可後續啟動重新識別（例：確認可歸責性時）。〝部分匿名及部分去連結〞意謂事先指定開啟者，且僅該指定開啟者，可識別該鑑別之個體。例：圖書館可能需要識別未歸還所借書籍之個體，以便發送逾期通知予該個體。目前之密碼學技術可用以提供部分匿名及部分去連結之鑑別。

CNS 29191 在去識別化過程中定義了 4 個角色：

- 核發者：核發信符予宣稱者之個體；
- 宣稱者：待查證者鑑別之個體；
- 查證者：查核宣稱者是否擁有有效信符之個體；
- 指定開啟者：可重新識別宣稱者之個體。

其框架於上述 4 個角色間，具有下列 4 項基本操作。

- 信符核發過程：核發者與宣稱者間進行信符核發之過程。完成本過程後，宣稱者始具有信符；
- 設置過程：指定開啟者設置對重新識別為必要之密碼式資訊的過程；
- 鑑別過程：宣稱者與查證者間，進行鑑別並產生鑑別紀錄單之過程。若查證者判定宣稱者持有有效信符，則鑑別成功；

- 重新識別過程：指定開啟者由鑑別紀錄單識別宣稱者之過程。於此過程中，指定開啟者使用鑑別紀錄單，且於適當時可使用其他資訊，進行重新識別。

部分匿名及部分去連結鑑別之框架，如圖 6 說明。

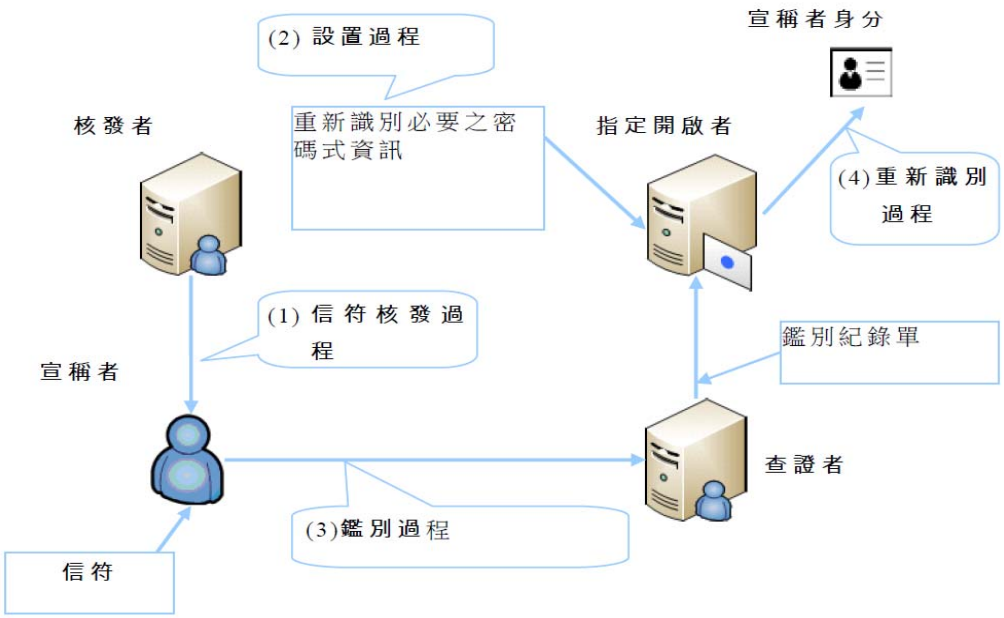

圖 6、部分匿名及部分去連結程序

資料來源：CNS 29191

CNS 29191 要求事項：

A. 宣稱者應由查證者鑑別，而不能由查證者識別。

對於向查證者保持匿名之宣稱者，其交易不應提供任何可用以識別宣稱者之資訊，但允許查證者證實宣稱者持有有效之信符。

B. 鑑別紀錄單本身不得提供能連結同一宣稱者多項鑑別交易之資訊。

對於向查證者保持不可連結之宣稱者，其交易不得提供可連結同一宣稱者履行之多項交易的任何資訊。

C. 鑑別紀錄單應包含供指定開啟者重新識別宣稱者之必要資訊。

為使指定開啟者之後能重新識別宣稱者，成功交易產生之紀錄單應提供識別宣稱者之資訊。注意，於適當情況下，指定開啟者可使用其他資訊以進行重新識別。

D. 指定開啟者應能提供所宣稱身分為正確之證據。

為避免指定開啟者之不誠實宣稱，指定開啟者應能提供重新識別程序已正當履行之證據。

(四) 通訊傳播事業巨量資料去識別化操作可行機制

1. 去識別化過程驗證機制之功能

所謂「驗證（Certification）」，係指對特定產品、過程或服務能符合一定要求，由中立之第三者出具書面證明之程序。根據「個人資料去識別化過程驗證要求及控制措施」PII 去識別化過程要求事項，組織應訂定符合一定要求之 PII 去識別化步驟，並依此進行去識別化。去識別化過程驗證機制之功能大致如下：

- 協助證明組織並無違反個人資料保護法之主觀的故意或過失；
- 協助證明組織已採行適當之安全維護措施；
- 協助證明個人資料遭違法蒐集或利用，非因組織違反個人資料保護法所致。

組織最終是否需負損害賠償責任，因為是由個案承審法院決定，故不能完全保證通過驗證即必然可免除損害賠償責任。驗證機制是在協助組織事前檢視其作業管理措施及流程，並保留相關紀錄資料，以備個案發生時用以強化其舉證能力，擁有較多的證據站在較有利的地位，降低損害賠償責任之風險。

2. 去識別化之程度與風險之關係

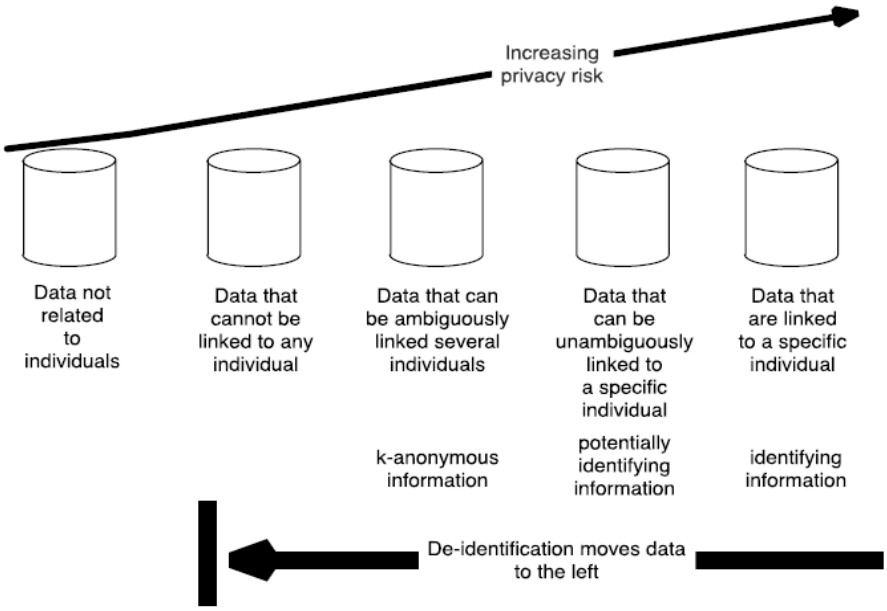

圖 7、去識別化之程度與風險

資料來源：美國標準技術局內部報告（NISTIR）8053

去識別化之程度愈高，風險愈低，而通常資料可用性亦愈低。而去識別化之程度愈低，風險愈高，然通常資料可用性亦愈高。

3. 風險分析方法

風險分析方法通常可分為：定量分析（quantitative analysis）、定性分析（qualitative analysis）及半定量分析（semi-quantitative analysis）。

- 定量分析：依據確實數值（金額、技術或人為尺度）表示之特定後果，以及風險之發生機率分析風險。進行此種分析方法通常很複雜，需研究及開發組織特定模型，故一般只應用於評估最顯著潛在風險。因難以達成期望之精確度，故可使用敏感性分析，測試不同考量之影響；
- 定性分析：使用文字及描述尺度評鑑所識別風險之相對大小；
- 半定量分析：將描述尺度之點轉換成數值評分（例如：“1”=罕見、“5”=十分肯定會發生；“1”=影響極微、“5”=影響嚴重）。雖此方法比定性分析產生更結構化的風險排序，但不宜依據比較相對風險（即，比較某風險與另一風險之衝擊）產生評分。

4. 隱私衝擊評鑑

隱私衝擊評鑑通常指對於 PII 處理之風險識別、風險分析及風險評估的整體過程。隱私衝擊評鑑為一項產出，其為風險管理之一部分，隱私衝擊評鑑乃專注於確保遵循隱私權及資料保護法規之要求，以及評鑑於新的或

大幅修改計畫或活動中的隱私權含意。

隱私風險是假想的情境，其描述風險源（例如：競爭對手通過收買員工）如何能於威脅全景（例如：濫用發送電子郵件）中，利用個人資料支援資產（例如：可操作資料之檔案管理系統），並造成個人資料（例如：客戶檔案）發生擔心的事件（例如：非法取得個人資料），因而對 PII 當事人的隱私產生影響（例如：不請自來的募捐、隱私侵犯之感覺等）。組織對於所有涉及個人資料之系統應進行隱私衝擊評鑑。風險係以其可能性（likelihood）及後果嚴重程度（severity）估算。

- 可能性表示發生風險的可能性。其基本上取決於支援資產面對威脅之脆弱性，以及風險源利用此等脆弱性的能力。
- 後果嚴重程度表示風險發生後，衝擊的大小。其基本上取決於潛在衝擊之不利影響。

隱私衝擊評鑑報告應至少包含下列內容：

- 簡介；
- 評鑑範圍；
- 隱私權要求事項；
- 風險評鑑（包含識別所有可能之隱私風險及衝擊等級與後果）；
- 風險處理（例如：符合法律及法規或最小化資料收集，以避免風險；實作各項資料保護控制措施，以降低風險；簽定契約條款或購買保

險，以轉移風險）；

- 依據隱私衝擊評鑑結果之結論（剩餘風險及決策）。

組織應依據隱私衝擊評鑑結果，實作 PII 處理生命週期各階段之各項控制措施，並定期稽核及審查其有效性。組織若進行 PII 去識別化過程，則應依據對 PII 去識別化過程之隱私衝擊評鑑結果，實作各項控制措施，並定期稽核及審查其有效性。隱私衝擊評鑑宜框限於更大範圍之組織風險管理框架內。

5. PII 資料去識別化後之重新識別風險計算

決定資料可識別風險之原則如表 5。

表 5、資料可識別風險判斷

原則	解釋	風險值範例
重現性（Replicability）	根據資料將持續連結至 PII 當事人之機率，將資料屬性定出風險等級之優先序。	低:病患之口腔疾病，會改變。 高:病患之牙齒照片相對穩定。
資源可用性（Resource Availability）	判定哪些外部資源含有特定個人之識別資料及資訊中之重覆特徵，以及何人被允許存	低:實驗室報告中之個人身分通常不會對實驗室外披露。 高:個人身分及人口資料往往出現於公共資源中，例：出

原則	解釋	風險值範例
	取該資源。	生、死亡及婚姻狀態。
區別性（Distinguish）	判定某 PII 資料可於資料集之中被區別出的程度。	低：估計在美國使用出生年、性別及郵遞區號前 3 碼之組合約有 0.04%機率可唯一識別某居民。意指僅經由此等資料之組合可識別特定居民之可能性低。 高：估計在美國使用出生日期、性別及 5 碼郵遞區號可唯一識別某居民之機率超過 50%。意指經由此 3 個資料之組合可識別一半以上的美國人。
評鑑風險（Assess Risk）	必須同時綜合考量重現性、資源可用性及區別性風險。重現性風險、資源可用性風險及區別性風險越高，資料被識別出之風險越高。	低：資料不具區別性，但其可能並未獨立重現，且很少於公眾可取用之多個人資料源中揭露。 高：人口資料具高度區別性、高度重現性並揭露於公共資源中。

可使用此等原則，判定資料集之中的 PII 資料去識別化後之重新識別風險值。

6. 經 PII 去識別化資料之重新識別驗證

組織應對擬公開之所有經 PII 去識別化資料進行〝重新識別測試〞，至少包含下列項目：

- 搜尋網頁，嘗試連結 PII 當事人；
- 搜尋全國或地方新聞資料庫，嘗試連結 PII 當事人；
- 搜尋政府單位或其他組織之開放資料，嘗試連結 PII 當事人；
- 以社群網路嘗試連結 PII 當事人。

因公眾可用之資料數量，隨時增長，故組織應定期重新對公開之經 PII 去識別化資料進行〝重新識別測試〞，以重新評鑑其風險。若發現其風險超過門檻值，組織應立即移除可能揭露個人隱私之資料，重新處理，並停止或修改（採取更嚴格之）去識別化過程。

(五) 國內發展現況

1. 公開資料去識別化規範

我國經濟部標準檢驗局於 2015 年 7 月制定「個人資料去識別化過程驗證要求及控制措施」規範，是世界第一部個人資料去識別化規範之國家。然此規範僅針對公開資料作去識別化過程驗證，並未對巨量資料之個人資料去識別化過程有所規範。

目前已有財政部財政資訊中心（104 年 11 月）、主計總處、衛福部、標準檢驗局（105 年 12 月），4 項個人資料去識別化過程通過驗證。驗證單位目前僅只有財團法人台灣電子檢驗中心。

2. TPIPAS 個人資料保護標章

臺灣個人資料保護與管理制度規範（Taiwan Personal Information Protection and Administration System, TPIPAS）是使組織以「PDCA 方法論」，建立一套將個人資料保護與組織營運連結之系統化管理制度。此規範係對於組織之個人資料管理制度進行內、外部評量及用以核發組織「資料隱私保護標章」（Data Privacy Protection Mark, DP Mark）之依據。

該規範目前的問題在於並未對風險管理進行詳細規範，而此恰好是現代管理系統驗證之核心所在，例如：改版後之 ISO 27001、9000、14000 皆為 risk-based 管理系統驗證。未來改版後將可更切合國內現況。根據其網站資料，截至 106 年 11 月，我國已有 20 個公司（單位）取得此標章。

第三節 比較分析

一、 先進國家個人資料保護機制比較

根據歐盟、美國、英國之個人資料保護規範，研究團隊初步以立法方

式、訊務資料、位置資料三面向進行初步分析，詳如表 6 說明。

表 6、先進國家個人資料保護機制比較

		歐盟	美國	英國
個人資料保護立法方式		• 1995 年「個人資料保護指令」，2016 修訂為「個人資料保護規則」，為個人資料處理原則。 • 2002 年「電子隱私指令」，2017 年修訂為電子隱私規則，規範通訊領域之個人資料隱私保護。	• 對於個人資料保護，美國尚未有一體適用之個人資料與隱私權保護規範，僅由不同產業領域訂定不同的規範方式。	• 1998 年「資料保護法」，為個人資料處理原則。 • 2003 年「隱私與電子通訊規則」，2011 年修訂，規範通訊領域之個人資料隱私保護。
訊務資料	定義	• 係指以電子通訊網路中通訊傳輸為目的、或為歸責目的而處理的資料。	• 「電信事業用戶基於電信服務契約而使電信事業取得有關其使用電信服務數、技術規格、型態、目的地與總額之資訊」，亦包括「客戶資訊相關的電話服務帳單資訊」，通常就是電信事業為提供服務時由用戶取得的資訊。	• 係指以電子通訊網路中通訊傳輸為目的、或為歸責目的而處理的資料。
	處理、利用範圍	• 當通訊傳輸目的不在時，必須被刪除或去識別化處理。 • 為用戶帳務與互連費用所需的訊務資料，得處理之，但必須是在對帳單提出異議或付款請求之期間內為限。 • 為行銷或加值服務之目的，若取得用戶或使用者的同意，於目的之必要範圍與期間內處理訊務資料，且應提供用戶撤銷同意之機會。	• 對於可被識別的個人資料，除法律規定或為了服務提供，以及公共利益考量或經客戶同意之外。電信服務業者僅能在提供（A）蒐集該資訊之特定電信服務，或（B）其他必要的相關服務（包含發行名錄）始得利用、揭露，或准許近用此類資料。	• 訊務資料必須在處理期限內予以刪除或去識別化。 • 在電子通訊行銷交易與訊務資料管理、客戶調查、詐欺預防與偵查、專為該用戶提供加值服務與電子通訊服務行銷的範圍內處理訊務資料。 • 在公眾電子通訊提供者親為或在其監督下，可以處理或儲存該個人資料當事人的訊務資料。

		歐盟	美國	**英國**
	告知義務	・所處理的訊務資料之類型。 ・為用戶帳務及互連費用之目的資料處理期間。 ・為行銷或加值服務目的，在取的同意前告知行銷必要的期間。 ・Cookies 使用 opt-in。	・1996 年電信法中並未規範告知義務，而是由 FCC 在 CPNI 規則中規範。CPNI 規則規定尋求客戶的同意必須伴隨告知客戶其 CPNI 的權利。FCC 規則對 opt-in 告知義務採取較彈性的方式，而對 opt-out 的告知義務採用嚴謹的標準。	・服務提供者須告知用戶處理資料的相關資訊、目的與持續時間。 ・在告知用戶 cookies 存放位置、用途與儲存資訊，且取得其同意後，始得使用 cookie 技術。
位置資料	定義	・位置資料係指在電子通訊網路中處理、得以表明公眾電子通訊服務使用者的終端設備所在地理位置。	置資料包括： ・有關商業行動裝置服務的通話位置資訊； ・自動當機時所通知的資訊。	・位置資料係指在電子通訊網路中處理、得以表明公眾電子通訊服務使用者的終端設備所在地理位置。
	處理、利用範圍	・只能在經匿名化或者須取得使用者或用戶的同意才能處理位置資料。 ・讓使用者及用戶有機會能隨時撤銷其先前之同意。 ・每一通訊傳輸時，暫時地拒絕位置資料的處理 （Article 9） 。	・須取得客戶事先明示授權使用無線位置資料。	・在個人資料當事人同意且有必要前提下，可將位置資料用於加值服務中。 ・位置資料可由服務提供者親為、在其監督下進行處理。 ・讓使用者及用戶有機會能隨時撤銷其先前之同意，服務提供者須提供撤銷同意資料處理的便利方法。
	告知義務	・欲處理的位置資料種類； ・處理的用途與時段； ・提供該加值服務時，位置資料是否會傳輸至第三方。	・須取得客戶事先明示授權使用無線位置資料。	・欲處理的位置資料種類； ・處理的用途與時段； ・提供該加值服務時，位置資料是否會傳輸至第三方。

依據各國個人資料保護法定義，個人資料一般係指可直接或間接識別特定個人的資料，亦即只有可識別個人的資料，才受到個人資料保護法規範。因此，若是資料已去識別化，或是匿名或遮蔽等方式，即不受個人資料保護法規範，可歸屬於非個人資料。

所謂「可識別至特定個人」之定義，目前各國間仍有許多模糊空間，以 IP 位址是否屬於個人資料為例，不同國家的法律認定就不盡相同。如歐盟，IP 位址是被視為可識別至特定個人的個人資料，美國聯邦貿易委員會（Federal Trade Commission, FTC）亦認為，若 IP 位址與醫療健康資訊有關，就會被認定為個人資料之一。

綜觀目前對於通訊傳播領域隱私保護的資料類型可概分為訊務資料與位置資料，訊務資料包含路由資訊、連線期間、連線時間與通訊流量等資料。位置資料可藉由使用者使用之終端設備，對照出所在位置的經緯度與海拔高度以判別行進路線與相關地理資訊，亦可利用網路單元細胞（Network Cell）之紀錄得知時間相關資訊。基本的個人資料保護與隱私維護原則可區分以下階段：

- 蒐集階段

個人資料蒐集應有適當限制，並須取得當事人的同意，避免過度

蒐集。

- 處理階段

資料處理係指將在個人資料編輯成為個人檔案（包括電子化或是人工建檔系統）的過程中，確保資料的正確性與完整，以及儲存資料的安全性。

- 利用階段：

確保個人資料利用符合當初蒐集時所告知的使用目的，並且限制只能在此範圍內利用。若變更不同用途時，得須重新取得當事人同意。

- 銷毀階段

個人資料過了保存期限，應予以銷毀，以降低資料外洩風險。

二、 國際主要去識別化技術

目前國際間去識別化技術依據數據性質不同而有不同方法，主要方法如表 7 說明。

表 7、去識別化技術

技術	說明	舉例
紀錄抑制（Record Suppression）	• 刪除資料，例如一個單元格或是一行，避免經由特定的特徵識別出相同群組的個人。 • 當準識別符（如性別、種族、郵遞區號）的組合公開呈現高度風險。 • 常用於公眾健康報告、地理空間分析。 • 可能會導致資料失真。	將個人資料的特定屬性排除，例如診斷碼或年齡組別中的人數少於 5 人。
抑制（Suppression）	• 將某一資料欄位（如罕見疾病）的資料值抑制或遮罩。	個人資料紀錄中包含一個罕見的值。
隨機（Randomization）	• 以隨機值取代直接識別符。 • 降低逆向識別的可能性。 • 常用於軟體測試建立資料集時，所有資料欄位都必須存在且具有實際價值。	隨機替換出生日期的演算法。
擾亂（Shuffling）	• 將資料中的一或多筆數值與其它的數值交換。	將隨機變數指配到個人資料資料中。
假名（Pseudonyms）	• 透過別名取代直接識別符，如同一水平的資料紀錄。	運用單向雜湊函數，雜湊函數可將一個值轉換成另一值的函數，但不可逆。
子取樣（Sub-Sampling）	• 隨機抽取一個資料集合。 • 使用分層確保資料變量的比例與原始的資料集合相同。	基於原始的資料集大小，隨機選取一取樣值，例如：10%。
聚合/概括（Aggregation/ Generalization）	• 將罕見的準識別符聚合至較大的資料集合。	將罕見的準識別符聚合，例如將居住人口較少的郵遞區號聚合到較大的地理區域。
增加雜訊（Adding Noise）	• 在連續的變量資料中加入雜訊或隨機值。	對資料添加亂數雜訊。
字元擾亂	• 重新排列資料中的字元順序	例如：SMITH 擾亂為 TMHIS

技術	說明	舉例
（Character Scrambling）	• 容易被逆向破解，並不可靠。	
字元遮罩（Character Masking）	• 資料值中的某一個字元或字元串替換成另一字元。	例如：將 SMITH 變更為 SMIT*或*M*T*。
截斷（Truncation）	• 將字元串中的某一字元刪除。	例如：SMITH 截斷為 MITH 或 SMIT 或 SITH。
編碼（Encoding）	• 以無意義的值取代資料。	SMITH 以 X&T%#取代。
模糊（Blurring）	• 降低數值的精確度。	將連續變量轉為分類資料或不同資料群組的聚合資料。
遮罩（Masking）	• 將某個資料集的原始值遮罩。	基於設定的遮罩原則，修改原始數據值。例如：年齡 18＋20。
擾動（Perturbation）	• 對數據進行微調，防止識別特定或稀有人群中的個人。	在各個資料單元中交換數據。

三、 去識別化機制比較

根據歐盟、美國、英國之去識別化相關守則，研究團隊初步以各國去識別化機制之目的與主要建議進行初步分析，詳如表 8 說明。

表 8、各國去識別化機制比較

	目的	主要規劃建議
歐盟	評估各種去識別化技術優缺點	• 定期評估是否存在新的風險，再鑑別（各種）剩餘風險； • 對於已確定的風險，評估已採取的措施是否足夠，並相應調整；

	目的	主要規劃建議
		• 監控和控制風險； • 針對剩餘風險，特別考量非匿名化資料與匿名化資料組合時，是否會發生重新識別。
美國	去識別化資料流向模型	• 資料釋出模式與管控方法 ✓ 釋出且遺忘模式 ✓ 資料使用協議模式 ✓ 飛地（Enclave）模式 • 去識別化及重新識別身分方法 ✓ 移除直接識別符 ✓ 假名化 ✓ 以連接攻擊重新識別身分 ✓ 準識別符之去識別化
英國	去識別化實作建議	• 個人資料開放流程； • 確定去識別化有效； • 個人資料與空間資訊之去識別化； • 去識別化之公開與限制存取； • 去識別化資料管理與風險評估。

去識別化技術藉由移除資料集內的可識別資訊，以保持所屬資料之可用性。各國均強調去識別化技術並非一定能確保個人隱私，進一步管控發布後的去識別化資料有其必要性，例如：資料使用協議，以管理限制資料接收者之行為。

目前各國對於重新識別當事人風險的認知仍相當有限，因為風險評估難以量化。從事分享個人資料之組織，應使用減緩重新識別當事人風險的方法，包含技術控制，例如：消除準識別符及其他可重新識

別個人資料當事人之資訊;持續檢視可能用以連結所分享或發佈之已去識別化資訊之資料;控制已去識別化資料,諸如資料使用協議與點擊同意協議,禁止重新識別當事人、連結其他資料或再分享予其他人;及限制資料接收者行為之技術控制措施。在去識別化議題日益引發關注之前提下,衡量個人資料與風險,仍需進一步的標準與技術。

各國及歐盟對於個人資料去識別化之法規、規則及作業規範,均未超出 CNS 29100 標準中之隱私原則範圍,且著重於規範評鑑、稽核與審查程序,並未要求及偏好特定之去識別化方法及風險評鑑方法。

第四節 本章小結

歐盟隱私保護法規係以個人資料保護規則為原則性立法,為保障自然人之基本權與自由,針對個人資料處理過程建立隱私保護標準。就個人資料處理「資料之品質原則」、「資料處理合法原則」、「敏感資料處理原則」及「告知當事人原則」,而其中關於個人資料當事人則另有「接觸權利」、「更正刪除或封存個人資料」以及「反對權利」等加以規範。而有鑑於通訊科技的變遷,歐洲議會於 2002 年通過「電子通訊個人資料處理暨隱私權保護指令」,為整個歐盟境內之電子通

訊確立新的規範框架，針對公共通訊網路，尤其是用戶個人資料自動儲存與處理能力，提供法律、管制政策與技術之特別規定。

美國隱私保護尚未有一致性之個人資料保護法規。就通訊傳播領域的個人資料保護，係依據服務類型的服務而有不同立法，以電信領域而言，1996 電信法第 222 條及 FCC 的 CPNI 規則為主要規範。而傳播領域，以 1984 年有線通訊政策法適用於有線電視服務。有線電視業者須善盡告知用戶對於其個人資料蒐集、利用、處理的義務，且蒐集資料的目的不存在時，有線電視業者應銷毀此等用戶個人資料。

英國隱私保護法規係以 1998 年資料保護法為原則性立法，針對個人資料之取得、儲存、利用與揭露等加以規範，同時訂定取得資料當事人同意與跨國界個人資料傳輸活動之原則。對於通訊領域個人資料保護，於 2011 年修訂「隱私與電子通訊規則」，規範內容著重用戶使用電子通訊服務之個人資料蒐集、處理、利用的保護，同時強化網路服務使用者之自主權，包括同意與撤銷。

依據前述國際實務經驗，除美國由各主管機關訂定所屬事業之個人資料或隱私保護外，歐盟與英國以「政府管制」方式整體性的規範個人資料與隱私保護的框架。歐盟設有電子隱私規則，英國設有「隱

私與電子通訊規則」，美國於各通訊傳播事業規範中設有個人資料隱私保護條款。目前我國也是採取「政府管制」方式整體性的規範個人資料隱私保護，再由各中央目的事業主管機關分別監理，對於通訊傳播事業個人資料保護法或法規命令，國內目前正在推動資通安全管理法草案、電子通訊傳播法草案訂定。

第參章　業者現況分析

本章節就業者自評、說明會與業者訪談之研究工作，分析業者現階段對於個人資料隱私保護與去識別化機制的規劃與實務做法。

第一節 業者自評

業者自評為第一次說明會後，請業者依公司對於自評表中的要求事項與控制措施，檢視內部的實際運作情形進行填覆，完整自評表內容請參見技術規範草案附件一說明。本計畫已收到中嘉網路股份有限公司、北都數位有線電視股份有限公司、全國數位有線電視股份有限公司、新彰數位有線電視股份有限公司、台固媒體股份有限公司、三大有線電視股份有限公司、新永安有線電視股份有限公司、凱擘股份有限公司、中華電信，共計 9 家業者回覆，部分業者為地區性系統台表示由總公司統一回覆。

自評表共區分 5 項要求事項，各要求事項又細分不同控制措施，業者依據控制措施說明，檢視公司內部實務運作情形，填覆自評結果，自評結果區分符合、不符合、部分符合、不適用之選項，其中不適用為公司環境中可排除的條件，例如：控制措施有個人資料國際傳輸的

要求，而公司沒有個人資料國際傳輸的行為，如此便不適用該控制措施。經綜整業者自評結果後，將符合程度區分為高、中、低，高代表該要求事項的自評結果多為符合或部分符合，而中代表多為部分符合或不適用，低則代表多為不符合，分析結果如表 9 說明。

表 9、業者自評分析

要求事項	符合程度	說明
隱私權政策	中	• 依個人資料保護法，實施個人資料隱私保護措施。 • 未制訂去識別化過程保護隱私之承諾及要求。
個人資料隱私風險管理過程	中	• 依個人資料保護法，實施個人資料隱私保護措施。 • 未有去識別化隱私衝擊評鑑控制措施與定期稽核。
個人可識別資訊之隱私權原則要求	高	依個人資料保護法，實作基本個人資料隱私保護措施。
個人資料去識別化過程之要求	低	多數公司未依照國際與國內個人資料去識別化標準，實行個人資料去識別化控制措施。
重新識別個人資料之要求	低	

一、 隱私權政策（符合程度：中）

目前業者均有訂定公司之隱私權政策，本要求事項以基本個人資料隱私權為主，其中控制措施 3.2 要求隱私權政策應包含對去識別化

過程保護隱私之承諾與要求，由於目前多數業者尚未依照國際與國內個人資料去識別化標準實施去識別化機制，故未將相關承諾及要求列入隱私權政策。

二、 個人資料隱私風險管理過程（符合程度：中）

目前業者均已訂定公司之個人資料隱私風險管理過程，但本要求事項中控制措施 4.1.4 要求業者進行個人資料去識別化時，應針對去識別化過程進行隱私衝擊評鑑，實作各項相關控制措施，並定期稽核及審查控制措施之有效性，由於目前多數業者尚未依照國際與國內標準實施個人資料去識別化機制，故未有去識別化過程之隱私衝擊評鑑與相關控制措施。

三、 個人可識別資訊（個人資料）之隱私權原則要求（符合程度：高）

依據自評結果，大部分公司已依據個人資料保護法要求，實施基本個人資料隱私保護，包括同意與選擇、目的適法性、蒐集限制、資料極小化、利用、保留及揭露限制、準確性及品質、存取限制等措施。

四、 個人資料去識別化過程之要求（符合程度：低）

本要求事項之控制措施以去識別化機制為主，主要控制措施如下說明。

- 個人資料去識別化過程的治理結構。
- 監督及審查個人資料去識別化過程之治理的安排。
- PII 去識別化過程之標準作業程序。
- 個人資料遭非預期揭露之災難復原計畫。
- 重新識別測試。
- 委外處理個人資料去識別化工作之要求。
- 對組織資料分析之要求事項。

由於目前多數業者尚未依照國際與國內個人資料去識別化標準實施個人資料去識別化機制，故在此要求事項中的自評結果以不符合居多，但個人資料遭非預期揭露之災害復原計畫一項，部分業者為符合，因為個人資料揭露之災害復原屬基本個人資料隱私保護一環，業者依個人資料保護法實施個人資料隱私保護機制時，已涵蓋了個人資料遭非預期揭露之災害復原計畫。

其次，也有少數業者填覆符合個人資料去識別化過程的相關要求，其主張為資料庫系統中是以機上盒智慧卡卡號或是MOD機上盒機號替代申裝戶個人資料，從資料庫系統並無法直接識別特定個人，實質

上已達到去識別化之效果。

五、 重新識別個人資料之要求（符合程度：低）

本要求事項之控制措施以重新識別個人資料為主，主要的控制措施如下說明。

- 經匿名（或擬匿名）處理後資料之接收者應僅能鑑別個人資料當事人之資料屬性，而無法識別出個人資料當事人。
- 同一個人資料當事人經匿名（或擬匿名）處理後的不同資料，不得提供具有聚合後能連結至該個人資料當事人之資訊。
- 資料經可逆之擬匿名處理後，應可於適當時（例如：法定之稽核），由個人資料控制者重新識別個人資料當事人。
- 於合法且有必要情況下（例如：法定之稽核），個人資料控制者應提供能正確重新識別個人資料當事人之證據。

由於目前多數業者尚未依照國際與國內個人資料去識別化標準實施去識別化機制，自然也無實施重新識別個人資料的機制，故在此要求事項中的自評結果以不符合居多。少數業者填覆符合重新識別個人資料之要求，其主張為機上盒智慧卡卡號或是 MOD 機上盒機號替代申裝戶個人資料，並無重新識別問題。

第二節 業者說明會

一、 第一次說明會

- 時間：106 年 8 月 16 日（星期三）下午 3 時 00 分
- 地點：國家通訊傳播委員會濟南路辦公室 7 樓大禮堂（臺北市濟南路 2 段 16 號 7 樓）
- 出席者（依首字筆畫數排序）：中嘉網路股份有限公司、中華電信北區分公司（MOD）、台固媒體股份有限公司、有線廣播電視系統經營者、台灣數位光訊科技集團、台灣寬頻通訊股份有限公司、台灣有線寬頻協會、財團法人電信技術中心、國家通訊傳播委員會基礎設施事務處、國家通訊傳播委員會北區監理處、國家通訊傳播委員會中區監理處、國家通訊傳播委員會南區監理處、國家通訊傳播委員會平臺事業管理處、凱擘股份有限公司
- 主席：國家通訊傳播委員會林慶恒簡任技正
- 研究團隊：蔡敦仁博士、蘇俊吉研究員、許博堯副研究員
- 簡報議題：
  - 本計畫目標

- 國際去識別化相關規範
- 我國去識別化發展與標準
- 交流與討論（依發言順序）

表 10、第一次說明會交流與討論內容

發言單位與答覆人	發言內容整理
台灣有線寬頻產業協會	1. 協會將協助研究團隊針對自評表填覆安排會議，邀請會員討論。 2. 去識別化議題，我們也關注許久，相信業界在個人資料保護法部分也有相關的因應作法，當我們要進行個人資料蒐集與處理行為，想請教有無突破的方法。
蔡敦仁博士	1. 規範旨在保護大家，個人資料蒐集、處理、利用如何做，大家其實都見仁見智，以法律面為例，101 年有民眾與台權會向衛福部提告，不希望衛福部把去識別化後的健保資料後提供給學者專家分析，該官司一直上訴駁回到今年一月份終於定案，最高行政法院判決駁回，表示去識別化有效性，未來如按照

	規範實施也通過檢查的話，若發生法律訴訟時，會站在比較有利的位置，等於是幫大家解決問題。此外規範也能將個人資料保護法不太明確的條文可操作化，也就是企業實施裡面的控制措施後，就符合個人資料保護法要求，甚至更嚴謹，因為法律條文往往讓企業明瞭限制，而規範有助於釐清法律面問題，法律如果有爭議，照判決，看是否有判決例子，若無判決例子，則看是否有相關權責單位的解釋函，所以在判決書中大量引用法務部的釋函，就個人資料如何蒐集、處理、利用，未來如能落實規範規定，不一定要通過驗證，如果能將規範內化，建設管理系統，留下證據，違反個人資料保護法的風險將會降至最低。 2. 如果貴公司有推行 ISO 27001 或 ISO 9001 品管、ISO 14000 再來實施去識別化，會比較容易達成，一樣要建立相關文件、組織，只是標的不同。此外，我們也建議要建立不同管理系統的聯合評鑑，例如：公司內部的資安系統應該與個人資料保護單位合併，不應該是兩

	個獨立組織，在資安單位內增加一項工作執掌或任務，設立一個人資料保護小組來執行，而不是重新發明整套個人資料保護機制。 3. 自評表中第三欄為公司內部管理的文件、規章、證據，檢查時會去查看這些資料是否存在。
中嘉網路股份有限公司	公司已導入 ISO 27001，自評表相關內容多以 ISMS 要求來填覆，基本上差距不大，或許有些不符合自評表要求，屆時再請研究團隊協助提出建議。
凱擘股份有限公司	本公司已導入 ISO 27001 等相關資訊安全管理程序，也包含相關的個人資料保護措施，將協助填覆自評表內容。
台固媒體股份有限公司	除 27001 外，也參考個人資料管理制度（PIMS）程序書，目前並沒有認證，後續會再視情況導入。
台灣寬頻通訊顧問股份有限公司	與中嘉情況類似，有導入 ISO 27001 自評表內的控制措施，有些目前沒有的措施，會再瞭解狀況。
世新有線電視股份有限公司與國興衛視	目前尚未導入 ISO 27001，但有配合 27001 控制措施實施個人資料保護，自評表內容，

	公司內部也會進行對應。
大台中數位有線電視	1. 本公司為前威達雲端電訊，針對剛提到的行政法院判決，駁回原告上訴，有關去識別化為合法，那是因為公益大於私利，因為國人十大死因都需要研究，所以需要很多的病歷資料，基於這樣的理由與其它因素，而駁回原告。 2. 我們公司有一類、二類電信、有線電視、衛星廣播等特許執照，我們公司從去年 12 月開始導入 ISO 27001、ISO 27011，於今年 5 月開始第一階段與第二階段稽核，並無缺失，也是由本人負責推動，針對自評表內容提及的組織從上位階概念來看是整間公司，但從產、銷、人、發、財，不同單位又有不同組織，每個組織若有不同受者與傳送者，所以要訂技術規範來看恐怕不是 20 多頁可以解決，且特許執照種類很多。 3. 個人資料保護法施行細則有規定要保護的對象是現在生存的自然人，以固網來說，辦理電路出租需要雙證件，採實

	名驗證，但如果是法人來辦，法人便不在個人資料保護法範圍內，就法規面並未規定要收取負責人雙證件，但是中華電信與遠傳電信卻要我們提供負責人雙證件，否則無法辦理，我要表達的意思是個人資料保護法是很上位階的概念，是原始於憲法裡人性的尊嚴，個人資料包含兩部分，第一個部分是隱性資料，如 DNA，是絕對保留，除非有特定目的、事由，才能蒐集，其它部分，請問各位同業，是否明瞭個人資料範圍，有哪些是個人資料？個人資料保護法訂的很抽象，但容許主管機關有解釋空間，但業者往往無法解釋，本公司的部分經營地區較偏僻，我們公司刷卡收費的不到 4%，有很多都是要人工收費，若要告知客戶對個人資料的認知，以及蒐集、處理、利用的程序，客戶往往會回答聽不懂，因此個人資料提供者無法在國家通訊傳播委員會的管轄範圍內去教育他。 4. 訂規範的目的在於保護個人資料提供者，但對於業者而言成本會很高，很多 ISO 條文看不懂，若國家通訊傳播委員

	會沒有定義細則，業者不像行政院，沒有強大的解釋資源、人才，我有辦法去解釋 ISO、法條，是因為我們受過嚴格訓練。技術規範定義時，國家通訊傳播委員會如果沒有定義細節的東西，會讓企業沒有一定標準，會始得公司推行的人自行猜測，若函文國家通訊傳播委員會尋求解答，時間上可能會拖很久，也不見得會很清楚，因為規範很多都是從原文翻過來的。因此，國家推行這個規範不是不好，但是要落實在每個地方、每個角度，而且能夠在業者跟個人資料提供者、國家法律遵循之間取得平衡，國家通訊傳播委員會是主管機關應該要定義細節性，才不會造成國家通訊傳播委員會標準與業者不一的情形，甚至是在定義規範後，仍應予與者個別溝通，畢竟每個業者環境情況不一。

蔡敦仁博士	1. 一般訂技術規範時，並不會只有條文，有一些比較技術性的控制措施，我們會提供實作指引，說明如何落實，自評表僅有控制措施與要求事項，在未來規範中會加入實作指引，讓大家可以參考，我們希望技術規範要有技術背景或專家才可以推行，實際上實行 ISO 精神為例，說你所做，做你所說，而非說一套做一套。當然推行標準認證會有成本發生，但也只有初次推行時，通過後只需要維持即可。 2. 有關個人資料安全意識問題，需強調的是企業從上到下都需要教育訓練，個人資料保護法概念需要清楚；至於對民眾，企業可基於善良本意，不侵犯民眾個人資料，蒐集時便不要蒐集非必要個人資料，蒐集極小化是重要的要求。 3. 至於個人資料保護法確實是保護自然人，法人非其範圍，也有其它法律保護營業的企業，例如營業秘密法等。個人資料保護法為普通法，如果有特別法，自然優先於普通法，如果有某些法律特別規定可蒐集特定個人資料自然優先。

	4. 剛提到的最高行政法院判例，個人資料保護法確實是以促進公眾利益為目的。
全國數位有線電視股份有限公司	如果委外個人資料隱私政策系統，要找什麼認證機構或主管機關可提供什麼指導。
蔡敦仁博士	有很多輔導顧問公司，例如三大會計師事務所，但費用較高，若有相關的認證輔導問題也可以來信詢問。
國家通訊傳播委員會陳炳華科長	1. 或許理論與實作會存在差距，日後推行時我們盡可能提供範例作參考，或許大家比較容易理解法規意涵與公司實際狀況，這樣或許執行起來比較容易。 2. 接下來會進行訪談業者，可主動聯繫研究團隊，或由研究團隊與業者接洽後約定訪談會議，再請業者多多配合，也可瞭解整體運作。 3. 如果貴公司有網頁的話，可以在網頁說明隱私權政策，也要提供用戶取消個人資料蒐集處理利用的選項，盡量做到資訊透明化，達到隱私保護的作用。
國家通訊傳播委員會林慶恒簡任技正	剛剛有提到有一些原則問題，個人資料蒐集到底是 Opt-In 或是 Opt-Out，若為 Opt-In 還要另外徵求同意，那問題會比較大，後續研

	究團隊會去釐清這些問題，依我們國內的法治現況，這樣的行為有沒有需要再額外同意，就通訊領域而言，有些規定較為嚴格，例如小額付費，會於合約書加註個人資料蒐集的同意徵求，後續若對執行面的可操作性，再請研究團隊進行研究，包括執行的人如何做，稽核的人如何稽核。做一些指引性的操作，對未來個人資料去識別化會有很大的幫助。

二、 第二次說明會

- 時間：106 年 10 月 27 日（星期五）下午 3 時 30 分
- 地點：國家通訊傳播委員會濟南路辦公室 7 樓大禮堂（臺北市濟南路 2 段 16 號 7 樓）
- 出席者（依首字筆畫數排序）：中嘉網路股份有限公司、中華電信北區分公司（MOD）、台固媒體股份有限公司、有線廣播電視系統經營者、台灣數位光訊科技集團、台灣寬頻通訊股份有限公司、台灣有線寬頻協會、財團法人電信技術中心、國家通訊傳播委員會基礎設施事務處、國家通訊傳播委員會北區監理處、國家通訊傳播委員會中區監理處、國家通訊傳播委員會南區監理處、國家通訊傳播委員會平臺事業管理處、凱擘股份有限公司

- 主席：國家通訊傳播委員會林慶恒簡任技正
- 研究團隊：蔡敦仁博士、蘇俊吉研究員、許博堯副研究員
- 簡報議題：
  - 通訊傳播事業個人資料去識別化技術規範草案說明
  - 交流與討論（依發言順序）

表 11、第二次說明會交流與討論內容

發言單位與答覆人	發言內容整理
台灣寬頻通訊顧問股份有限公司	技術規範在 11 月底定稿後會進行後續的程序，在定稿後是否會成為強制性規範，如果是一定要遵守的規範，但公司內部並沒有要進行資料分析行為，是否僅遵守個人資料隱私保護的部分即可，而去識別化部分則不適用。
國家通訊傳播委員會陳炳華科長	就第一個問題說明，我們所知道有很多 MSO 都有做收視調查，如有類似分析行為，就要做去識別化，若無收視調查，則要保護好客戶個人資料，如果有個人資料外洩的情事，處分會很重，也可能涉及刑責的部分，技術規範在未來會列入審驗技術規範，

	基本上會區分兩個部分，基本的部分適用未進行收視調查的情形，就好像基礎設施一樣，會請業者提報 CIIP 的作業規範，因此也希望藉由本計畫案說明會、業者訪談提供技術規範草案內容的討論空間，如果有窒礙難行的措施，也希望業者能趕快提出，避免在技術規範草案內容底定後，再出現無法實施的聲音出現。
中華電信北區電信分公司	現場與會多為有線電視業者，但目前個人資料蒐集很多是手機或是網路上的廣告等服務，因此想瞭解此規範的效力範圍如何界定？
國家通訊傳播委員會陳炳華科長	目前會先針對有線電視與 MOD 兩部分，若涉及電信部分，NCC 平臺處目前也正在進行委託研究，針對客戶服務品質與營運要求來探討，本計畫僅針對技術部分來處理。
中嘉網路股份有限公司	無意見，未來將配合主管機關辦法實施。
凱擘股份有限公司	1. 在去識別化部分有沒有時程上的規劃？業者導入去識別化機制時，是由業者自行建置，或是 NCC 有輔導單位，哪些單位可進行驗證？ 2. 業者自行找認證單位通過去識別化認

	證，是否就符合 NCC 規範要求，另外是否可說明實施時程？
國家通訊傳播委員會陳炳華科長	1. 關於驗證由業者自行找，輔導部分則是盡量比照 ISO27001，提供相關的範本供參考，因為每個單位內部組織環境與運作皆不相同，業者需自行評估有哪一些內部組織涉及個人資料與分析，本計畫的技術規範是指技術的部分，只針對有進行收視調查的行為會進行規範，有關客戶資料部分則由營運平臺處規劃，ISO27001 為自願性規範，未來本草案內容若列入審驗規範，則具有強制性，當然若未進行收視調查，機上盒也未回傳用戶個人資料，就沒有實施去識別化機制的必要性。 2. 關於實施時程，NCC 會給業者實施緩衝期，在認證單位部分，若有找公正第三方進行認證，NCC 一樣會承認。部分有線電視業者因資本額較小，本計畫訂技術規範時會更具體，讓業者能依據規範內容更容易施作，或許可節省認證的成本。若未來規範正式發佈，也會再召開說明會進行說明。

台固媒體股份有限公司	無意見。
新彰數位有線電視	無意見。
北都數位有線電視	無意見。
全國數位有線電視股份有限公司	目前與客戶簽訂之契約已有個人資料蒐集、處理、利用的聲明，在規範制訂後，這部分是否具回溯的效力，對於已簽約的客戶在技術面上要如何處理？
蔡敦仁博士	個人認為就技術規範而言，業者仍須審視契約上的聲明與規範條文是否有落差，若有落差還是要補起來。
新北市有線電視	目前無收視率調查，若未來實施，會配合主管機關。
大豐有線電視	目前業者多有開發 APPs 等業務，相關業務可能也有個人資料蒐集與分析行為，此部分是否也需要考量納入去識別化機制，因為有可能不做收視率調查，但 APPs 服務確有相關的個人資料蒐集與分析行為。
蔡敦仁博士	此部分也要納入去識別化機制，因為網路服務上通訊傳輸，個人資料等敏感性資料也要加密或進行去識別化才會相對安全。

國家通訊傳播委員會陳炳華科長	1. 收視調查區分兩部分，一部分是巨量資料對全體客戶進行分析，一部分是精準行銷，針對用戶的使用習慣，以後比較敏感的部分會是精準行銷的部分，客戶會覺得個人資料完全由業者掌握，曾經有一案例，機上盒有故障，由業者告知機上盒都未開機，客戶會覺得業者端怎會知道用戶的使用行為，不管客戶有無使用寬頻上網服務，但機上盒本身就有開啟小頻寬的回傳機制。 2. 先前契約的個人資料聲明是否溯及既往，另一個方法也可以使用網頁的方式告知，但用戶與業者之間往往是誠信原則，例如 Google 也有被懲處的案例，業者本身還是要確實遵守規範內容。
國家通訊傳播委員會林慶恒簡任技正	在規範內容部分有部分屬於大方向的原則，部分條文有詳細的說明，未來規範內容會盡量加註相關指引。
國家通訊傳播委員會平臺事業管理處	今年也有委託資策會進行個人資料保護相關研究，明年會進行業者的個人資料保護自評與自我檢視，同時也會開設個人資料保護的相關課程，以及進行稽核的動作。

國家通訊傳播委員會陳炳華科長	建議各位回去後，將技術規範草案內容提供給公司內部的工程或資安相關單位，因為現場與會的大都為法務單位，未來實行時，可能與工程部門息息相關，資安人員也能從旁提供專業建議，屆時規範發佈時，才不至於出現不同的意見。

三、 說明會意見與答覆整理

(一) 提高業者落實技術規範之可操作性

訂定技術規範其目的在於保護個人資料提供者、但就法規或技術規範的條文定義往往很抽象，容許較大的解釋空間，卻造成產業遵循實行時的困擾、包括成本與人才等因素，因此規範若缺乏細節性，將始得產業界自行猜測、解釋。

從國家法規面而論，法規條文有其法源位階與效力，較高位階的法規與命令一般會較抽象，而本技術規範草案將針對規範中的條文要求，例如：一些技術性的控制措施加註實作指引或範例說明。

(二) 技術規範之範圍與適用性

技術規範草案內容涵蓋了個人資料隱私保護與去識別化的相關要求，業者提出未進行個人資料分析行為時，只須遵循個人資料隱私

保護相關控制措施。

技術規範草案內容可區分基本的個人資料隱私保護與去識別化兩部分，然而部分有線電視與 MOD 業者已進行收視行為調查，若有相關的分析行為，除適用基本個人資料隱私保護外，也須遵循去識別化的相關要求。

(三) 行動應用服務之去識別化適用性

近年來，有線電視業者為增加營收提升競爭力，紛紛規劃創新商業模式，例如：OTT 影音、行動影音等服務，相關服務也存在個人資料蒐集與分析行為，因此，是否也適用個人資料隱私保護與去識別化之規範。

新型態行動影音應用服務其性質與有線電視服務與 MOD 服務有異，行動影音應用服務用戶多為申請服務之特定個人，收視人以申請服務之個人為主；而有線電視服務與 MOD 服務則為特定家戶，收視人則為該家戶或申請住所的居住人，若進行收視行為分析，其參考價值更高，因此行動影音應用服務也須進行個人資料隱私保護與去識別化，因為網路服務上通訊傳輸，個人資料等敏感資料也須加密保護或

去識別化才會相對安全。

第三節 業者訪談

一、 訪談對象與時程規劃

為達到瞭解產業界在個人資料保護與去識別化機制實務操作之目的，本計畫於第一次說明會後，協請台灣有線寬頻產業協會提供有意願接受訪談之有線電視業者名單與窗口，共計 5 間。另包含經營 MOD 服務之中華電信股份有限公司。訪談對象涵蓋資通訊、法務、管理部相關部門，詳細訪談對象與時間，如表 12 說明。

表 12、訪談對象

公司名稱		部門	與談人	訪談時間
有線電視業者	中嘉網路股份有限公司	數位及資訊部	林立章經理	106.09.29
	台灣寬頻通訊顧問股份有限公司	法務暨法規部	張聖怡經理	106.10.11
	天外天有線電視	管理處	張鴻隆經理	106.10.11
	大豐有線電視	數位視訊組	林俊凱主任	106.10.12
	凱擘股份有限公司	資訊管理處	陳治平處長	106.10.17
		法務/法規室	梁逸琪管理師	

MOD	中華電信股份有限公司	北區電信分公司新媒體處	林志弘處長 王麗凱管理師	106.10.17

二、 訪談議題

訪談議題區分三部分，訪談內容(有線電視業者)如表 13 說明，有線電視業者訪談稿與 MOD 服務訪談稿請參見附件三。

表 13、訪談內容

項次		問題
資料蒐集與儲存	1.	對於使用服務的個人，貴公司所蒐集個人資料有哪些？
	2.	貴公司提供服務時，儲存/歸檔何種資料？（如：收視頻道、收視時段、收視時間、帳單明細等）？
	3.	是否提供互動性服務？蒐集之個人資料有哪些？儲存/歸檔何種資料？例如MOD服務訂閱影集、購物服務之購買物品等。
	4.	請說明問題1、2、3的回覆資料的儲存時限，依據的標準為何？
	5.	若貴公司根據預先訂定的時限儲存資料，當該時限屆滿時，貴公司作何處理？這方面貴公司有什麼規定的程序？
用戶權利與資料利	6.	貴公司是否就問題1、2、3所列儲存的資料，徵求用戶的同意？以何種方式徵求用戶同意？如不徵求用戶同意，請說明儲存這些資料的法律依據。
	7.	貴公司是否根據問題1、2、3的答覆所指的資料歸納整理用戶概況？如果是，為何目的？對何種資料進行處理？是否徵求用戶的同意？
	8.	如果貴公司除提供有線電視服務外，還提供其它服務，是否與該等服務共享貴公司透過有線電視服務蒐集的資料？反之是否亦然？如果是這樣，請說明共享的資料。
	9.	貴公司如何就個人資料的蒐集、處理及儲存等事項知會用戶？是否就諸如個人概況、收視偏好的歸納整理及其它互動活動的等事項向用戶提供資訊？

項次		問題
用	10.	貴公司是否給用戶以查閱權及更正權，並按其要求更正、刪除與封存個人資料？
去識別化與資料控制	11.	貴公司是否對個人資料作去識別化處理？如果是，請說明具體做法（如使用何種技術？）。如何確保不可逆？已作去識別化的資料包含何種資訊？
	12.	個人資料之存取權限？資料電子化過程時，員工是否有相關安全管控措施？
	13.	貴公司是否向第三方傳送資料？請說明與以下哪些類型的公司分享。 • 數據分析公司； • 廣告商； • 子公司； • 其它- 請說明。
	14.	貴公司在個人資料保存是否採取安全措施？採取哪些措施？

三、 訪談結果綜整

(一) 資料蒐集與儲存

第一部分為資料蒐集與儲存，旨在瞭解產業界提供使用者申辦服務與使用服務時所蒐集的資料，包括個人資料與間接的服務使用行為資料，以及資料蒐集後的保存方式與程序。

1. 所蒐集之個人資料

經訪談與業者提供之服務申裝表單中使用者資料欄位得知所蒐集個人資料包括：客戶姓名、市內電話、行動電話、裝機地址、收費地址、大樓（社區）名稱、戶籍地址、身分證正反面影本、健保卡/

駕照影本、電子郵件。

部分業者開發之 MOD 行動應用服務，安裝服務註冊帳號時，需填覆電子信箱、登入密碼、暱稱、性別（非必填）、手機號碼，此外，若以信用卡付費便要填覆信用卡卡號，若以紙本帳單也要再填覆收件人姓名、地址，此部分會因行動裝置之作業系統而不同，部分作業系統有特定的收費平臺，例如：由 Apple 公司的 Apple Pay 付費，便不需要再填覆付費的相關個人資料。

其它的蒐集資料方面，使用 MOD 行動應用服務的用戶 IP 位址只會於 Log 中記錄，並不會儲存在資料庫系統中，其目的在於鎖定台灣用戶，因為影片有地區授權。用戶行動上網的 IP 位址多為浮動 IP，能代表的位置資訊也並不精確，只有在測試或查修服務時才會確認 IP 位址。因此，對業者而言，IP 位址並非是分析商業價值的資料。

2. 提供服務時蒐集之資料

目前有線電視業者普遍提供隨選視訊服務（Video On Demand, VOD），該服務毋須申請寬頻網路服務，業者會於機上盒開啟通訊埠，用戶即可觀看視訊內容與使用加值服務，加值服務一般包括天氣、路

況資訊、股市、購物等服務。VOD 服務可蒐集資料包括訂閱頻道、點擊影片、包月方案、加值服務使用紀錄、遙控器行為。

(二) 用戶權利與資料利用

第二部分為用戶權利與資料利用，旨在瞭解產業界在蒐集、處理、利用資料時，是否有提供使用者行使其權利的選擇，包括同意、查閱、更正等權利，以及資料利用的方式與目的。

1. 用戶權利

業者通常會於服務申裝表單載明個人資料蒐集、處理、利用條款，並由申裝用戶同意後進行簽章，若是 MOD 行動應用服務則於軟體安裝後，註冊帳戶時加註個人資料蒐集、處理、利用條款，提供使用者點選同意或不同意之選項；在資料保存時限方面，依照個人資料保護法規定：「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。」保存用戶個人資料。個人資料查閱、更正、刪除權由用戶於線上或臨櫃辦理，經核對身分無誤後始得行使。

2. 資料利用

VOD 服務蒐集使用行為資料主要有拆帳與服務優化兩目的。由於需支付影片權利金，因此經由統計用戶點選的頻道與影片來計算業者需支付給影片供應商的權利金，例如包月 199 每月有 50 片影片，每部影片的權利金不是用 50 片平均分攤，而是依據實際收視的影片來拆帳，用戶在觀看超過所設定之時間才會列入拆帳計算。

服務優化可區分為遙控器行為與影片點擊數統計，在遙控器行為部分，以北部與南部收視戶為例，北部收視戶偏好數字選台，後端系統會記錄該用戶喜歡看哪個頻道，將該用戶常看的頻道置入一個優先的傳輸串流（Transport Stream,TS）中，而南部收視戶則將幾個連續頻道同一個 TS，一個 TS 可存放幾個頻道，也就是在同一個正交振幅調變（Quadrature Amplitude Modulation, QAM），Tuner 不需切換，節省用戶切換節目時的時間感受，提供用戶更優化的服務品質。其次，在影片點擊數統計方面，業者通常會統計影片點擊數，再整理成熱門影片排行榜，提供用戶參考。

多數受訪業者均表示目前沒有進一步進行收視行為分析，有部分業者內部正在規劃收視行為分析的方法，且表示有線電視收視戶的收

視行為，並無法辨識特定個人，而是整個申裝戶中的所有收視戶，其次，前述提到的點擊數與相關資料在系統中均以機上盒的智慧卡號碼連結，只有少數的資料庫系統有完整的用戶個人資料，例如帳務系統。中華電信表示其MOD服務已於公司資料分析部門進行收視行為分析，但分析部門所接收收視行為資料只對應到 MOD 機上盒機號，不會是特定的個人資訊，而 MOD 機上盒機號也不能代表特定個人，僅能代表一申裝戶中所有收視戶的收視行為，已具備去識別化之作用。

分析系統、工務系統、帳務系統彼此間不會連接，所保存的資料也不會相同，分析系統與工務系統一般不儲存用戶個人資料、而帳務系統不會有收視行為等資料。若是因為查修或是證據保留等因素，需查詢申裝用戶個人資料，則須經由業者內部之申請程序查詢。

(三) 去識別化與資料控制

第三部分為去識別化與資料控制，旨在瞭解產業界在去識別化的實務經驗，以及對於資料的安全控制措施。在去識別化機制方面，大部分業者均表示尚未進行數據分析，因此未依照國際與國內的個人資料去識別化標準建立去識別化機制，對於中華電信 MOD 服務所進行的收視行為分析與有線電視業者統計影片點擊數的行為，中華電信表

示分析部門與分析人員僅能從系統上看到MOD機上盒機號與有線電視機上盒智慧卡卡號，無法經由資料識別出申裝用戶。

在資料控制方面，可分為存取權限、電子化過程、資料分享、資料保存控制來說明：

1. 存取權限

申裝用戶相關資料經電子化建檔後將儲存於資料庫，同時進行資料檢核作業，確認申裝用戶資料與服務內容正確性。資料庫系統將連結各業務資訊系統，主要會有客服、帳務、工務系統，三種系統皆設有存取權限，只有相關人員才能存取，同時能查閱的資料也不盡相同，例如：工務系統只能查閱有線電視智慧卡卡號與MOD機上盒機號所對應的資料，無法看到申裝用戶個人資料；客服系統通常需核對申裝戶基本資料，能存取的權限往往較大，一般會於客服作業電腦上安裝安全稽核軟體。各系統台有各自的報表權限，無法跨系統台存取。所有帳號存取權限設定都須業者內部透過表單申請經由最高長官簽核，每半年要審核帳號有效性。

2. 電子化過程

臨櫃辦理之申裝用戶資料將於現場電子化建檔，臨櫃客服人員透過遠端連線到用戶資料系統，相關資料並不會儲存到客服人員所使用的電腦上，臨櫃客服與線上客服的每通電話都會進行錄音，線上預約與網路預約則於工務人員裝機與啟用服務後將申裝工單與服務契約攜回，由資料建檔人員進行電子化作業，工務單位、工務人員與資料建檔人員都須簽具資料保密協議，同時資料建檔環境會建置保密機制，包括攝影機、電腦存取權限設定，或是安裝作業安全存錄軟體等，監視有無不當之操作行為，例如下載大量個人資料、異常頻繁登入等。

3. 資料分享

由於多數受訪業者表示目前未有資料分析行為，中華電信 MOD 服務也未委託第三方進行資料分析，因此就資料分析部分並無資料分享。現階段主要的資料分享案例有二，一是申裝服務與障礙排除時，若業者委託第三方廠商，則會給第三方廠商申裝工單，此情形無法避免不提供申裝用戶個人資料，包括姓名、電話、裝機住址等，因此一定會與第三方廠商簽訂保密切結，同時合作契約也會載明申裝工單等包含用戶個人資料的文件，也要再施工完後繳回業者的條文，若未繳

回需要承擔相對的法律責任與罰則。

第二個資料分享的情形是有線電視業者的MOD行動應用服務可與家中的機上盒進行綁定，綁定的目的在於將MOD行動應用服務所收視的影片費用列入有線電視帳單中，因此會有個人資料共享情形。

此外，比較特別的是有線電視業者多系統經營者（Multiple System Operator, MSO）其下屬的地區系統台，每個系統台只能存取本身的的用戶個人資料與產出整體報表，只有總公司擁有全部系統台的用戶資料，並無儲存用戶相關的收視行為資料。

4. 資料保存控制

在資料保存方面，業者會定期進行資料保存演練（多為一年一次），每天備份，部分多系統經營者具備資料庫異地備援機制，資料異動時會同步至遠端，同時也會進行異地備援演練，防火牆、交換機備援演練。在系統維護方面，若有委外維護情形，受委託廠商每次都須申請VPN 連線，廠商帳號設定正常維護的最小化權限。資料庫系統一般會安裝安全稽核軟體，所有存取行為，如開啟、儲存、瀏覽、列印、下載，都會進行存錄，若有異常操作行為則馬上提出告警，例如：廠

商請求超出其權限的大量資料。

第四節 通訊傳播事業個人資料儲存與處理流程

本計畫於進行有線電視業者與 MOD 業者訪談後，初步整理通訊傳播事業個人資料儲存與作業流程，如圖 8 說明。此流程可區分服務申裝與契約簽定、電子化建檔、紙本資料入櫃上鎖、存入資料庫與資料檢核五階段流程，業者在不同階段設有不同安全機制，確保個人資料保密性。

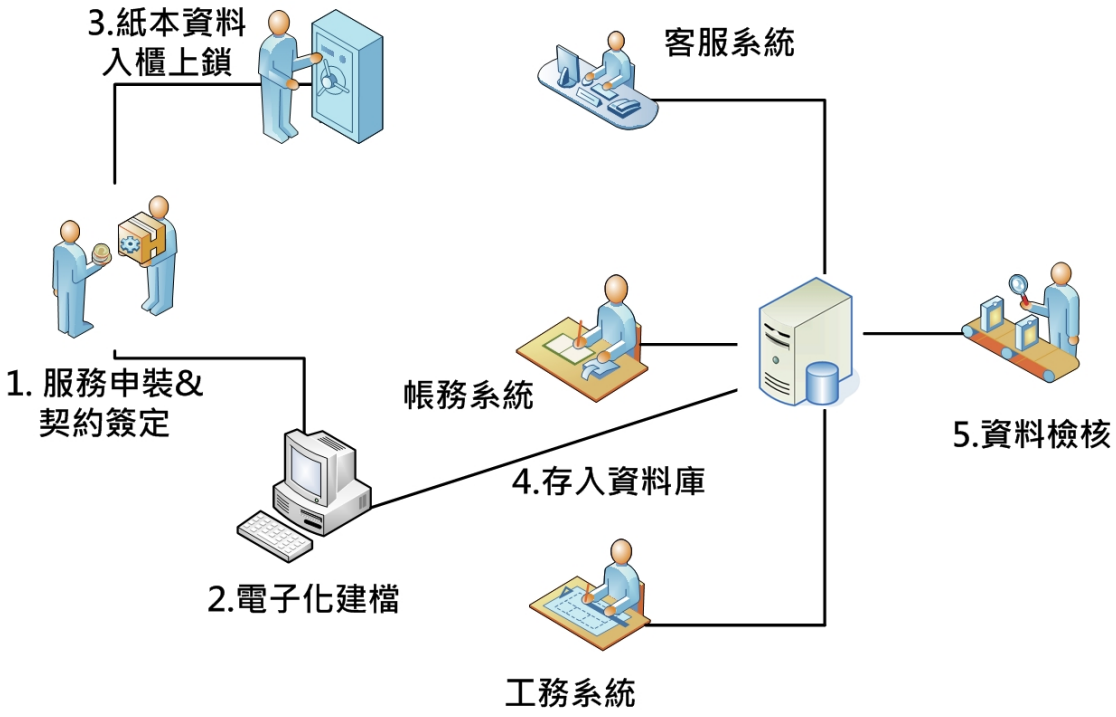

圖 8、通訊傳播事業個人資料儲存與處理流程

一、 服務申裝與契約簽定

1. 有線電視

有線電視業者提供民眾申裝時，會有線上預約、網路預約、臨櫃辦理申裝三種管道，業者收到民眾申裝需求後，將依據民眾提供的基本資料：姓名、電話、安裝地址，由工務單位至民眾住所進行裝機與啟用服務作業，線上與網路預約申裝將由工務人員於現場檢核申裝民眾身分，並收取申裝民眾雙證件影本，同時請民眾檢視申請服務與契約內容，申裝工單上會載明個人資料蒐集、處理、利用條款，待民眾確認且同意後，於申裝工單與服務契約進行簽章。

2. MOD 服務

MOD 服務提供網路與臨櫃辦理兩種申裝方式，民眾於網路申裝時，需於網頁填寫訂單，填寫訂單時會檢核申裝住所是否具備寬頻網路服務，同時填覆申裝用戶之基本資料，由工務單位至民眾住所進行裝機與啟用服務作業，工務人員將請民眾提供雙證件影本，檢核是否為申裝民眾本人，同時請民眾確認申請服務與契約內容，申裝工單會載明個人資料蒐集、處理、利用條款，待民眾確認且同意後，於申裝

工單與服務契約進行簽章。臨櫃辦理則於現場檢核雙證件，繳交雙證件影本，並簽定服務契約後，再由工務單位至申裝住所裝機與啟用服務。

二、 電子化建檔

臨櫃辦理之申裝用戶資料將於現場電腦以遠端連線方式進行電子化建檔，線上預約與網路預約申裝則於工務人員裝機與啟用服務後，將申裝工單與服務契約攜回，由資料建檔人員進行電子化作業，工務單位、工務人員與資料建檔人員都須簽具資料保密協議，同時資料建檔環境會建置保密機制，包括攝影機、電腦存取權限設定，或是在作業電腦上安裝作業安全存錄軟體等，監視有無不當之操作行為，例如下載大量個人資料、異常頻繁登入等。

三、 紙本資料入櫃上鎖

紙本資料將由文件管理人員至入文件檔案櫃，同時上鎖，只有指定的文件管理人員才能開鎖，相關紙本文件依個人資料保護法規定，於公司內部作業規範訂定保存期限，超出保存期限將進行銷毀動作。

四、 存入資料庫與資料檢核

申裝用戶相關資料經電子化建檔後儲存於資料庫，同時進行資料檢核作業，確認申裝用戶資料與服務內容正確性。資料庫系統將連結各業務資訊系統，主要會有客服、帳務、工務系統，三種系統皆設有存取權限，只有相關人員才能存取，同時能查閱的資料也不盡相同，例如工務系統只能查閱有線電視智慧卡卡號與MOD機上盒機號所對應的資料，無法看到申裝用戶個人資料；客服系統通常需核對申裝戶基本資料，能存取的資訊往往較大，一般會於客服作業電腦上安裝安全稽核軟體，避免異常的操作行為。

第肆章　技術規範草案架構

第一節 適用對象與架構

一、 適用對象

本技術規範適用於擬管理其隱私保護管理制度及個人資料去識別化過程的通訊傳播業者，尤其是下列業者。

- 多媒體內容傳輸平臺服務經營者：係指由固定通信業務經營者透過多媒體隨選系統（Multimedia On Demand, MOD）平臺，提供媒體隨選視訊內容、應用內容等多媒體內容服務之經營者。
- 有線廣播電視系統經營者：依有線廣播電視法定義之有線廣播電視系統經營者。
- OTT（Over The Top）服務經營者：指在未有服務品質保證的網路環境下，直接提供用戶各種視訊內容、語音通訊等服務之經營者。

二、架構說明

技術規範草案共 7 節，規範架構如圖 9 說明。詳細的規範內容請參見附件一，其中目的與用語及定義兩節，說明本規範目的，以及相關的名詞、定義，後五節定義不同的要求事項，以及詳細可操作的控制措施。

圖 9、「通訊傳播事業個人資料去識別化技術規範」架構

要求事項會區分兩部分，一為隱私保護基本要求，另一為去識別化過程要求，如表 14 說明。在隱私保護基本要求部分，不論是否有要做巨量資料分析或個人資料去識別化，所有的通訊傳播業者都適用，

涵蓋的節次為第 3 節第 1 部分、第 4 節第 1 部分、第 5 節，若業者有將資料交由第三方或是單位外部進行資料分析行為，則須符合去識別化過程之要求事項，涵蓋的節次包括第 3 節第 2 部分、第 4 節第 2 部分、第 6 節、第 7 節。

表 14、要求事項分類

要求種類	適用對象	節次
隱私保護基本要求	所有通訊傳播事業	第 3 節第 1 部分、第 4 節第 1 部分、第 5 節
去識別化過程要求	擬進行資料分析者（並據以行銷）	第 3 節第 2 部分、第 4 節第 2 部分、第 6 節、第 7 節

第二節 要求事項與控制措施概述

在實務操作方面，由於每間企業的系統環境與條件不一，因此在稽核前，業者需填覆適用性聲明，其目的在於釐清規範中有哪些要求事項不適用該公司環境，可以條列在適用性聲明中，例如有些要求事項為委外的控制措施，但該公司並無委外情事，只要稽核單位認為合理且同意，即可將此要求事項排除在稽核事項外，因此並不是所有的控制措施都要遵循。以下為控制措施初步說明。

一、 隱私政策

第一部分

1. 建立隱私政策（11 項控制措施）

組織之高階管理階層，應依營運要求及相關法律與法規，建立隱私政策，提供隱私保護之管理指導方針及支持。

第二部分

1. 去識別化（4 項控制措施）

組織若進行個人資料去識別化，則隱私政策應包含對去識別化過程保護隱私之承諾及要求。

2. 資料分析（3 項控制措施）

組織若自行、授權或委託第三方進行含有個人資料之資料（尤其是巨量資料）的分析工作，則隱私政策應包含對資料分析過程保護隱私之承諾及要求。

二、 個人資料隱私風險管理過程

第 1 部分（3 項控制措施）

1. 個人資料處理生命週期風險管理過程

2. 隱私衝擊評鑑

3. 依隱私衝擊評鑑實作控制措施

第 2 部分（2 項控制措施）

1. 依隱私衝擊評鑑實作個人資料去識別化控制措施

2. 依隱私衝擊評鑑實作資料分析控制措施

三、 個人資料之隱私原則要求

本節屬隱私保護基本要求，所有業者無論其是否要進行去識別化或使用涉及個人資料之資料進行分析，皆須符合本節之要求。

1. 同意及選擇（11 項控制措施）

2. 目的適法性及規定（3 項控制措施）

3. 蒐集限制（6 項控制措施）

4. 資料極小化（4 項控制措施）

5. 利用、持有及揭露限制（7 項控制措施）

6. 準確性及品質（6 項控制措施）

7. 公開、透明及告知（5 項控制措施）

8. 個人參與及存取（5 項控制措施）

9. 可歸責性（8 項控制措施）

10. 資訊安全（8 項控制措施）

11. 隱私遵循（4 項控制措施）

四、 個人資料去識別化過程之要求

本節屬個人資料去識別化過程要求，適用於擬進行個人資料去識別化，俾進行資料分析工作（及據以行銷）之通訊傳播事業。

1. 組織應建立有效且周延之個人資料去識別化過程的治理結構（7 項控制措施）。

2. 組織之高階管理階層應監督及審查個人資料去識別化過程之治理的安排（7 項控制措施）。

3. 組織應訂定個人資料去識別化過程之標準作業程序，並依此進行個人資料去識別化工作（6 項控制措施）。

4. 組織應備妥對個人資料遭非預期揭露之災難復原計畫（3 項控制措施）。

5. 組織應備妥程序，對已移除個人資料之揭露資料，依可接受風險，定期進行重新識別測試（5 項控制措施）。

6. 委外處理個人資料去識別化工作時，組織應監督、監視及稽核委外處理活動（8 項控制措施）。

7. 組織若對含有個人資料（巨量）之資料進行分析工作，應妥善保護隱私及設計資料分析機制（14 項控制措施）。

五、 重新識別個人資料之要求

本節屬個人資料去識別化過程要求，適用於擬進行個人資料去識別化，俾進行資料分析工作（及據以行銷）之通訊傳播事業。

1. 經匿名（或擬匿名）處理後資料之接收者應僅能鑑別個人資料當事人之資料屬性，而無法識別出個人資料當事人（1 項控制措施）。

2. 同一個人資料當事人之經匿名（或擬匿名）處理後之不同資料，不得提供具有聚合後能連結至該個人資料當事人之資訊（1 項控制措施）。

3. 資料經可逆之擬匿名處理後，應可由個人資料控制者重新識別個人資料當事人（5 項控制措施）。

4. 於合法且有必要情況下（例如：法定之稽核），組織應提供能正確重新識別個人資料當事人之證據（2 項控制措施）。

第伍章　未來推動建議

通訊傳播事業於建構個人資料保護系統之際，通常需要考量服務型態、經營規模、建置成本等諸多因素，企業往往因此望而遠之。經考量前述因素，本計畫擬訂之通訊傳播事業去識別化技術規範草案涵蓋個人資料保護與去識別化兩部分，提供通訊傳播事業彈性依循，相關控制措施依據業者條件不同而有選擇，以本計畫有線電視業者為例，部分業者為地方系統業者，其經營規模與服務型態與多系統經營者存在差異，例如：部分公司有個人資料傳輸與分享、統計分析行為，在實作控制措施上必然會有所不同；本技術規範草案依循國際標準組織（International Organization for Standardization, ISO）「說你所做」、「寫你所說」、「做你所寫」原則，通訊傳播事業於實作個人資料保護去識別化控制措施時，只須依據本身經營條件，選擇合理的要求事項與控制措施，經主管機關或第三方驗證機構稽核後，再納入個人資料保護去識別化作業範圍，有效提供技術規範的可操作性。

第一節 推動依據

我國個人資料保護法「依其揭露方式無從識別特定當事人」之用語，以及個人資料保護法施行細則「以代碼、匿名、隱藏部分資料或

其他方式，無從辨識該特定個人者」之用語，並無明確定義資料去除個人資訊後提供再利用之概念架構。

以英國資料保護法為例，於條文第 51 與 52 條中敘明權責機關應以促進產業實施去識別化機制為目的，制訂實務操作守則，該守則雖不具備法律效力，但可提供產業遵循的指導原則。本計畫將以此為參據，建議於通訊傳播事業相關管理辦法中新增去識別化相關規定。

第二節 建議法規規範內容

本建議法規規範內容係依照我國通訊傳播事業相關管理辦法進行規劃，適用對象為本計畫研究標的：有線電視業者、MOD 業者與 OTT 業者，建議於有線廣播電視系統工程技術管理辦法中新增法規規範內容，內容為個人資料保護及個人資料保護去識別化規定。

一、 個人資料保護

通訊傳播事業應遵循個人資料保護法、個人資料保護法施行細則，落實個人資料保護管理制度，保障個人資料當事人權利，並防止個人資料被竊取、竄改、毀損、滅失或洩漏，建立安全、可信賴之服務。

二、 個人資料去識別化

1. 通訊傳播事業應遵循個人資料保護法第 19 條、第 20 條，針對利用行為所設定的例外規定：「非公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人」。

2. 依據個人資料保護法施行細則第 17 條解釋，所稱無從識別特定當事人，指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者。

3. 通訊傳播事業實施去識別化作業，應依循以下原則：

(1) 採取合理、適當之去識別化措施；

(2) 於企業內部不同事業或部門之去識別化資料傳輸，須約定不還原去識別化資料；

(3) 提供去識別化資料予企業以外第三方時，須訂立契約禁止該第三方還原資料。

4. 通訊傳播事業實施合理、適當之去識別化措施，得依循通訊傳播事業個人資料去識別化技術規範草案。

建議法規規範內容僅為督促產業遵循之依據，實施細節與作業程序仍須參照本計畫擬訂之技術規範草案。

名詞釋義

中文名稱	英文名稱	說明
選擇退出	opt-out	先提供服務予使用者，再由使用者決定是否退出使用。
選擇加入	opt-in	先不提供服務予使用者，而由使用者決定要用後再啟用。
個人可識別資訊	Personal Identifiable Information	所有資訊其能用以識別此類資訊所涉之 PII 當事人，或係或得以直接或間接連結至 PII 當事人。
識別	Identification	使用 PII 當事人所宣稱之屬性或所對其觀察之屬性，由一組個體中挑選出某特定個人之過程。
去識別化	De-identification	採取一組合理之步驟，移除識別資料與個人資料當事人間之關聯的過程。
直接識別資料	Direct Identifying Data	直接識別 PII 當事人之資料。直接識別資料係不需額外資訊或經由交互連結公開資訊中之其他資訊即可用以識別 PII 當事人之資料。例：身分證號碼、指紋等。
間接識別資料	Indirect Identifying Data	僅於與其他間接識別資料一起使用時方足以識別 PII 當事人之資料。例：郵遞區號、生日、年齡等。

匿名性	Anonymity	不允許個人可識別資訊（PII）當事人被直接或間接識別之資訊特性。
匿名化	Anonymization	個人可識別資訊（PII）不可逆地變更之過程，以此方式，始得無法直接或間接識別 PII 當事人。
匿名資料	Anonymized data	個人可識別資訊（PII）經匿名化過程輸出所產生之資料。
擬匿名化/假名化	Pseudonymization	應用於個人可識別資訊（PII），以別名替換個人識別資訊之過程。
不可逆性	Irreversibility	由可識別至擬匿名之任何轉換狀況，其由擬匿名追踪回原始識別符是不可行的。
去連結資料	Unlinkable data	僅包含難以由熟練的分析師以合理工作量連結至 PII 資料。
重新識別	Re-identification	將已去識別化資料與原 PII 當事人重新建立關聯的過程。
K-匿名性	K-Anonymity	若發佈之資料中所包含之 PII 當事人的資訊與至少 K-1 個人的資訊，無法區別。
PII 當事人	PII principal	個人可識別資訊（PII）所關聯之自然人。

PII 控制者	PII controller	判定個人可識別資訊（PII）處理之目的及方法的隱私權相關者，而非就個人目的使用資料的法人或自然人。即指負責蒐集及管理個人資料之組織。
PII 處理者	PII processor	代表 PII 控制者並依其指示，處理個人可識別資訊（PII）之隱私權相關者。
PII 處理生命週期	PII processing life cycle	包含 PII 之蒐集、移轉、使用、儲存、移除等階段。
推論控制	inference control	控制僅揭露無法據以推論出原 PII 當事人之資料
公眾電子通訊提供者	Public Communications Service Provider	以電子方式傳輸資訊的服務提供者。
資訊公署	Information Commissioner’s Office	英國為維護公眾資訊權而設立之獨立政府機關，致力於提倡政府資訊公開及個人資料與隱私保護，為英國 1998 年資料保護法（Data Protection Act 1998）之主管機關。
資料處理者（受託者）	Data Processor	資料控制者依契約關係授權進行資料處理者。

資料控制者	Data Controller	指控制與負責在電腦或結構化文件中保存與使用個人資訊的自然人或法人。
個人資料當事人	Data Subject	與個人資料關聯的自然人。
建檔系統	Filing System	任何涉及個人的一組資訊，非以自動化控制設備相關建檔系統進行處理，但資訊內容依個人或個人評量標準相關之方式建構，始得該筆個人有關資訊容易被取得或揭露。
可被識別/足資識別	Identifiable	一個可以透過識別符（identifier），例如：姓名、識別號碼、位置資料（location data）、線上識別符（online identifier），或經由其他一項或多項身體、生理、基因、精神、經濟、文化或社會身分特徵，直接或間接識別自然人。
位置資料	Location Data	指在電子通訊網路中處理、得以表明公眾電子通訊服務使用者的終端設備所在地理位置。
線上識別符	Online Identifier	由裝置、應用程式、工具或網路協定所賦予的唯一識別符。
隨選視訊服務	Video On Demand, VOD	讓使用者透過網路選擇自己想要看的視訊內容的服務。用戶選定內容後，隨選視訊系統可以用串流媒體的方式進行即時播放。

多系統經營者	Multiple System Operator, MSO	指一擁有多家有線電視子系統台法定股權之經營者。
美國國家弱點資料庫	National Vulnerability Database	美國政府專門用來收集各種資訊系統安全漏洞和弱點資料的資料庫網站。

參考文獻

[1] 范姜真嫩，「我國電信業及電信加值網路業個人資料保護與監管機制之研究」，國家發展委員會編印，2015 年 4 月。

[2] 廖雪君，「以英國通訊傳播法之研訂及推動為典範，研究我國匯流法制定與推動之可行方向」，104 年公務人員出國專題研究報告書，2015 年 11 月 25 日。

[3] 國家發展委員會，「通訊傳播事業個人資料保護之機制及管理模式」，2015 年 4 月。

[4] 行政院經濟建設委員會，「服務業科技應用之個人隱私權保護 相關法制之研究 －以通訊傳播為中心」，2004 年 12 月。

[5] 法務部，「公務機關利用去識別化資料之合理風險控制及法律責任」，105 年 1 月 22 日。

[6] 財團法人資訊工業策進會，「主要國家政府開放資料（Open Government Data）機制與作法追蹤觀察報告（二）—英國」，103 年 12 月。

[7] 法務部，個人資料保護法，104 年 12 月 30 日。

[8] 法務部，個人資料保護法施行細則，105 年 3 月 2 日。

[9] 國家通訊傳播委員會，電信法，96 年 7 月 11 日。

[10] 國家通訊傳播委員會，電子通訊傳播法草案總說明，104 年 10 月 21 日。

[11] 經濟部標準檢驗局，CNS 29100「資訊技術-安全技術-隱私權框架」，103 年 6 月 4 日。

[12] 經濟部標準檢驗局，CNS 29191「資訊技術－安全技術－部分匿

名及部分去連結鑑別之要求事項」，104 年 6 月 4 日。

[13]經濟部標準檢驗局，個人資料去識別化過程驗證要求及控制措施，104 年 6 月 4 日。

[14]Cable Television Consumer Protection and Competition Act of 1992. Available at https://transition.fcc.gov/Bureaus/OSEC/library/legislative_histories/1439.pdf

[15]CSA, Big Data Security and Privacy Handbook: 100 Best Practices in Big Data Security and Privacy, 2016.

[16]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[17]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector （Directive on privacy and electronic communications）. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

[18]ENISA, Privacy by design in big data：An overview of privacy enhancing technologies in the era of big data analytics, 11/2015.

[19]Proposal for an ePrivacy Regulation, 10/01/2017. Available at https://ec.europa.eu/digital-single-market/en/news/proposal-regulatio

n-privacy-and-electronic-communications

[20]Reform of EU data protection rules, 14 April 2016. Available at http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[21]Data Protection Act 1998. Available at http://www.legislation.gov.uk/ukpga/1998/29/contents

[22]The Privacy and Electronic Communications （EC Directive） Regulations 2016. Available at http://www.legislation.gov.uk/uksi/2016/524/pdfs/uksi_20160524_en.pdf

[23]Telecommunications Act of 1996. Available at https://www.fcc.gov/general/telecommunications-act-1996

[24]Notice of Proposed Rulemaking on broadband internet service provider. Available at https://www.paulhastings.com/publications-items/details/?id=1c1ce969-2334-6428-811c-ff00004cbded

附件一 通訊傳播事業個人資料去識別化技術規範草案

通傳事業去識別化技術規範(草案)

國家通訊傳播委員會

中華民國 106 年 11 月

前言

新型態的通訊傳播應用服務具有多元化、互動、客製化等特性。其中使用巨量資料分析進行精準行銷，更是具有龐大的潛在商機。而通訊傳播業者除應依個人資料保護法(以下簡稱個資法)保護客戶資料外，巨量資料分析更可能涉及使用用戶之身分、位置、消費明細、使用行為、收視紀錄等個人資料。即使於利用時已移除相關個人資料，有心人可能仍可在巨量資料中找到關聯性，得以識別特定當事人。

通訊傳播業者蒐集之客戶個資，依蒐集特性可分為一次性(one-time)(例如：申請服務個資)及持續性(ongoing)(例如：手機發話位置)，而個資處理位置可能為個人載具、資料傳輸及蒐集網路、業者自有設施及第 3 方平台。

通訊傳播業者利用個人資料，僅限於與用戶簽訂之服務契約範圍，且除服務契約不可侵犯個資法所規定的基本權利外，並需實作使客戶可行使其基本權利(如：授予同意及撤回同意)之機制。另依法務部之見解，若組織將保有之個人資料，運用各種技術予以去識別化，而依其呈現方式已無從識別特定個人者，即非屬個人資料，而非個資法之適用範圍。故業者於利用巨量資料分析進行行銷前，應將資料進行去識別化。

個資去識別化之行為係定性為個資法第 2 條第 4 款所稱之〝處理〞。依個資法第 2 條第 1 款有關個人資料之定義的反面解釋可知，所謂〝個資去識別化〞，係指透過一定程序之處理，使資料無法直接或間接識別個人。此處所稱得以間接方式識別，依據個人資料保護法施行細則第 3 條規定：「指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人」。

個資法之體系架構係將〝蒐集〞及〝處理〞行為規範於相同法定要件之下，蓋個人資料之〝蒐集〞大多緊密伴隨著〝處理〞行為，故個資法並未特別區隔兩者之行為要件，且因去識別化資料須達到無從直接或間接識別特定人之程度，故去識別化之加工處理並未增加對當事人權益之額外侵害。因此，如原先蒐集個人資料之行為符合個資法第 19 條之規定，應可認為去識別化之處理並未逾越原先蒐集之特定目的（並非與原特定目的不相容），而得依據原先蒐集時之同一合法事由為之。

壹、目的及適用對象

本技術規範旨在使通訊傳播業者能建立隱私保護管理制度，保護其所蒐集、處理、利用之個資。並可供意圖建立個資去識別化過程(personal information deidentification process, PIDIP)之業者，用以管理對其所控制之個人可識別資訊(personal identifiable information, PII)進行去識別化之過程。而通常經去識別化過程處理之資料，可供後續利用。

本技術規範可供通訊傳播業者業者內部負責規劃、建立、實作及維護隱私保護管理制度及 PIDIP 者使用，並提供共同基礎，供負責管理個人資訊之管理階層使用，提升其對組織之隱私保護及去識別化過程之信心。本技術規範並可供通訊傳播業者組織內部及外部評鑑者使用，使其能對隱私保護管理制度及資料去識別化過程之要求事項與良好實務作法之遵循性有效評鑑。

本技術規範適用於擬管理其隱私保護管理制度及個資去識別化過程的通訊傳播業者，尤其是下列業者。

(1)多媒體內容傳輸平臺服務經營者：係指由固定通信業務經營者透過多媒體隨選系統(Multimedia On Demand, MOD)平臺，提供媒體隨選視訊內容、應用內容等多媒體內容服務之經營者。
(2)有線廣播電視系統經營者：依有線廣播電視法定義之有線廣播電視系統經營者
(3)OTT(Over The Top)服務經營者：指在未有服務品質保證的網路環境下，直接提供用戶各種視訊內容、語音通訊等服務之經營者。

本技術規範第三節及第四節，各分為 2 部分，第 1 部分為隱私保護要求，第 2 部分為擬進行資料分析(及據以行銷)之通傳事業組織需符合的個資去識別化過程要求。第五節屬隱私保護要求，而第六節及第七節屬個資去識別化過程要求。

貳、用語及定義

(1)可歸責性(accountability)：確保或能展示遵循隱私原則及資料保護原則(或法律要求)。
(2)匿名化(anonymization)：個人可識別資訊(PII) 不可逆地變更之過程， 以此方式，使得無法直接或間接識別 PII 當事人。
(3)匿名資料(anonymized data)：個人可識別資訊經匿名化過程輸出所產生之資料。
(4)稽核(audit)：系統性、獨立且文件化之過程，用以獲取稽核證據並客觀評估，以確定稽核準則所達到之程度。
備考 1. 稽核可為內部稽核(第一方)或外部稽核(第二方或第三方)，且可為聯合稽核(組合 2 或多個領域)。
備考 2. 〝稽核證據〞及〝稽核準則〞定義於 CNS 14809 中。
(5)能力(competence)：人員應用知識及技能以達成所欲結果之能力。
(6)同意(consent)：個人可識別資訊(PII)之當事人對於處理其 PII，依自由意志提供、特定及被告知之同意。
(7)矯正措施(corrective action)：用以消除不符合事項之原因，並防止再次發生的措施。
(8)去識別化(de-identification)：採取一組合理之步驟，移除識別資料與個資當事人之連結的過程。
(9)差分隱私(differential privacy)：於資料集查詢結果注入隨機〝雜訊〞，保證於數學上資料集之中的任一當事人個資之存在將被遮蔽之方法。此係個資去識別化方法之一類。通常需以軟體估算查詢之隱私風險，並決定於釋出資料之前應注入查詢結果之雜訊等級。
(10)識別(identification)：使用個資當事人所宣稱之屬性或所對其觀察之屬性，由一組人中挑選出某特定個資當事人之過程。
(11)直接識別資料(direct identifying data)：直接識別個資當事人之資料，此係不需額外資訊或經由交互連結公開資訊中之其他資訊即可用以識別個資當事人之資料。
例：身分證統一編號、指紋等。
(12)間接識別資料(indirect identifying data)：僅於與其他間接識別資料一起使用時方

足以識別個資當事人之資料。

例：郵遞區號、生日、年齡等。

(13)推論控制(inference control)：控制僅揭露無法據以推論出原個資當事人之資料。

(14) k-匿名性(k-anonymity)：發布之資料中所包含之個資當事人的資訊與至少 k-1 個人的資訊無法區別。

(15)選擇加入(opt-in)：過程或政策型式，據此，在同意就特定目的處理其個人可識別資訊(PII)之前， 要求個資當事人採取行動以進行明確表達。

(16)選擇退出(opt-out)：過程或政策型式，據此，就特定目的處理其個人可識別資訊(PII)之後，要求個資當事人採取行動以進行明確表達退出。

(17)個人可識別資訊(personally identifiable information, PII)：所有資訊其能用以識別此類資訊所涉之個資當事人，或係或得以直接或間接連結至個資當事人。

[來源：CNS 29100]

(18)PII 當事人(PII principal)：個人可識別資訊(PII)所關聯之 PII 當事人。

(19)政策(policy)：管理階層所正式表示之組織意圖及方向的聲明。

(20)隱私加強技術(privacy enhancing technology, PET)：隱私控制措施，包括資通訊技術(ICT)措施、產品或服務，於無損於 ICT 系統功能性下，藉由消除或減低個資，或藉由預防非必要及/或非所欲之個資處理，以保護隱私。

備考 1. PET 的範例包括(但不侷限於)消除、減低、遮罩或去識別化個資， 或預防非必要、未經授權及/或非所欲個資處理等之匿名化與擬匿名化工具。

備考 2.遮罩化為隱匿個資元件之過程。

(21)隱私政策(privacy policy)：由 PII 控制者正式表示， 於特別設定下處理個資相關之整體意旨及方向、規則與承諾。

(22)隱私原則(privacy principle)：一組共享價值，於資通訊技術系統下處理個資時，據以管理隱私保護。

(23)隱私取捨(privacy preference)：由 PII 當事人所為，就特定目的，有關其個資宜如何處理之特定選擇。

(24)隱私風險**(privacy risk)**：不確定性對隱私之影響。

備考 1. 在 CNS 14889 及 CNS 31000 中，風險定義為〝不確定性對目標之影響〞。

備考 2. 不確定性係缺乏(或部分缺乏)對事件、其後果或可能性之瞭解或知識相關資訊的狀態。

(25)隱私風險評鑑(privacy risk assessment)：關於個資處理之風險識別、風險分析及風險評估的整體過程。

備考：此過程 亦稱為隱私衝擊評鑑

(26)隱私保全要求事項(privacy safeguarding requirements)：組織在處理關於個資隱私保護之個資時，必須考量之 1 組要求事項。

(27)隱私利害相關者(privacy stakeholder)：與個資處理有關之決策或行動，可影響或受影響、或感知自身受影響的自然人或法人、權責機關、機構或任何其他團體。

(28)PII 之處理(processing of PII)：對 PII 履行之運作或 1 組運作。

備考： PII 處理運作之範例包括(但不侷限於)PII 之蒐集、儲存、修改、檢索、諮詢、揭露、匿名化、擬匿名化、散播或以其他方法使其可利用、刪除或銷毀。

(29)過程(process)：相互關聯或相互作用之活動的集合，其將輸入轉換為輸出。

(30)隱私衝擊評鑑(privacy risk assessment, PIA)：系統化的應用管理政策、程序及實務作法於隱私風險之溝通、諮詢、建立全景，以及識別、分析、評估、處理、監視及審查的過程。

(31)擬匿名化(pseudonymization)：應用於個資，以別名替換個人識別資訊之過程。又稱為〝假名化〞。

備考：參照 CNS 29100 之 4.4.4 擬匿名化資料。

(32)重新識別(re-identification)：將已去識別化資料與原個資當事人重新建立關聯的過程。

(33)合成資料(synthetic data)：由原資料集產生完全由〝虛構〞或變更識別之個資所組成之資料集。只要資料集之中的個資當事人數量夠大，即可保有原始資料集之統計特性，同時能提供差分隱私之數學雜訊保證。

(34)去連結資料(unlinkable data)：僅包含難以由熟練的分析師以合理工作量連結至個資之資料。

參、隱私政策

第 1 部分：隱私保護基本要求

3.1 建立隱私政策

目標：組織之高階管理階層，應依營運要求及相關法律與法規，建立隱私政策，提供隱私保護之管理指導方針及支持。

3.1.1 隱私政策要求事項(必備)

控制措施：組織之隱私政策應如下：

- 符合相關法律與法規要求及組織之營運要求。
- 敘明組織之高階管理階層對隱私保護之管理指導方針及支持。
- 敘明組織蒐集、處理、儲存、利用、刪除及銷毀個人資料之適法性及及相關措施。
- 界定組織蒐集、處理、儲存及利用個人資料之範圍。
- 敘明組織對含有個資之資料的存取管控，以及使用紀錄、軌跡資料及證據保存、稽核之規定與機制。
- 敘明含有個資之資料，保存之格式、方法、期限及相關保護措施，以及保有個資之特定目的消失或期限屆滿時之處置。
- 敘明組織之隱私利害相關者。
- 提供下列隱私管理事項之框架，並設定目標：
  - ●隱私管理審查委員會之組成、職掌及召開時機。
  - ●各工作小組之組成及任務。
  - ●認知宣導及教育訓練要求。
  - ●隱私保護之稽核要求。
  - ●對系統實施隱私衝擊評鑑之要求。
- 敘明隱私事宜之通報及應變機制。
- 敘明委外處理含有個資之資料的契約要求及對委外廠商之稽核要求。
- 敘明對隱私政策持續改善之承諾。

－使各隱私利害相關者可適時且容易取得。

3. 1.2 書面載明隱私政策並傳達(必備)

控制措施：組織應以書面載明其隱私政策，並有效及適時傳達予隱私利害相關者。

3. 1.3 隱私政策審查時機(必備)

控制措施：隱私政策應依規劃之期間或發生重大變更時審查，以確保其持續的合宜性、適切性及有效性。

3.1.4 依隱私利害相關者補充規定(選項)

控制措施：隱私政策應依不同隱私利害相關者，補充規定對應之詳細個資處理規則及義務。(例:針對接觸或利用個資之各特定部門或員工，訂定對應之管控程序。)

3.1.5 實作程序、存取控制、告知條款、稽核要求(必備)

控制措施：隱私政策應敘明設置哪些用以實作符合隱私政策之程序、存取控制、告知條款、稽核要求等。

3.1.6 內部隱私政策(必備)

控制措施：對內之隱私政策應載明組織採用之隱私保護目標、規則、義務、懲處規定、限制及/或控制措施，以滿足與組織個資處理生命週期各階段相關之隱私保全要求事項。

3.1.7 外部隱私政策(必備)

控制措施：組織應傳達予外部隱私利害相關者下列資訊：

－組織之名稱及辦公室地址，以及個資當事人可取得額外資訊之連絡窗口。
－所有相關之個資處理者的名稱。
－將蒐集之個資類別。
－蒐集個資之特定目的及適法性。
－個資利用之期間、領域、對象及方式。
－關於移轉個資至個資處理者之作法。
－個資保護之實務作法聲明及其目的。
－個資當事人得自由選擇提供個人資料時，不提供將對其權益之影響，以及選擇加入及之後選擇退出之機制。
－個資當事人對其被蒐集之個資的法律權利。
－提供個資當事人行使權利之機制，包含：

- 依當事人之請求，就蒐集之個人資料，答覆查詢、提供閱覽或製給複製本之機制。
- 依當事人之請求，更正或補充資料之機制。

3.1.8 違反隱私管理後果認知(必備)

控制措施：組織應備妥措施，使相關人員(尤其是個資處理者)認知違反隱私政策或安全要求之可能後果，包括：

－對個資處理者

- 委外處理者：法律責任、賠償、業務喪失、品牌或聲譽之損害等。
- 內部處理者：懲處、賠償等。

－對員工及約用人員：懲處、賠償等。

－對個資當事人：造成身體、物質、隱私及情緒等傷害。

組織並應建立正式程序，以因應違反隱私政策之行動。

3.1.9 認知宣導及教育訓練(必備)

控制措施:組織應每年定期對蒐集、處理或利用含有個資之資料的所有員工、約用人員、委外廠商人員及隱私利害相關者進行認知宣導及教育訓練。

3.1.10 定期內部稽核(必備)

控制措施：組織應每年定期實施隱私保護、個資去識別化及涉及個資之資料分析的內部稽核。

3.1.11 委外處理含有個資之資料(選項)

控制措施：組織若委外處理含有個資之資料，則委外處理廠商應遵循組織之隱私政策及要求事項。委外處理廠商應依據組織之隱私政策及要求事項，訂定相對應之隱私保護制度與控制措施。組職並應監督並定期及不定期稽核委外處理廠商之作業。組職應訂定資料移轉及於資料處理完畢後歸還及移除資料之作業程序，並監督廠商遵循。

第 2 部分：個資去識別化過程要求

3.2 個資去識別化之政策要求事項(選項)

目標：組織若進行個資去識別化，則隱私政策應包含對去識別化過程保護隱私之承諾及要求。

3.2.1 對外聲明

控制措施：組織若進行個資去識別化過程，隱私政策應包含下列項目，並應對外公布適宜之相關內容。

- 敘明組織之去識別化作法，並以一般用語描述將使用哪些去識別化技術及其產出。
- 敘明經去識別化資料之可能重新識別風險，以及組織決定接受風險之原則。
- 敘明去識別化資料之釋出原則。包含何種資料會公開、何種資料會對哪些特定對象有限揭露、或何種資料會供組織或他方利用，並敘明對應之相關風險、如何衡量與取捨、考量或未考量哪些因素、原因為何。

3.2.2 選擇適宜去識別化作法

控制措施：組織應依含有個資之資料的敏感性，針對不同資料釋出對象、應用及環境，規定適宜之〝隱私保護之私密資訊使用模型〞，並選擇適宜之去識別化作法。

3.2.3 重新識別測試及風險評鑑

控制措施：組織於利用、開放、揭露或移轉經去識別化資料前，應對資料進行〝重新識別測試〞及風險評鑑。

3.2.4 資料揭露控制

控制措施：組織若對公眾公開或對特定對象揭露經去識別化資料，應告知資料開放或揭露對象，使用此等資料之相關義務、責任、限制及風險，以及不當使用或移轉此等資料應負之責任及可能後果。並應要求資料揭露對象簽署資料使用切結書。

實作指引：對公眾之資訊公開透明，可增加公眾對組織之信任度，然基於資訊安全之考量，為不助長重新識別風險，組織應衡量是否需移

除所公布之風險評鑑報告等文件中之某些資訊，或僅公布其彙總報告。

實作指引：適宜之去識別化作法及保護措施，可能包含：離群值之處理，以及隨機化方法、差動隱私、k-匿名性、l-多樣性、t-閉合性等推論控制方法。

實作指引：〝隱私保護之私密資訊使用模型〞(model for privacy-preserving use of private information)通常分為 2 種：

－隱私保護資料探勘(privacy preserving data mining, PPDM)模型：於此模型中，資料控制者不提供原始資料予使用者，而是將資料使用於統計處理或機器學習。處理結果可依彙總及聚合以統計表格之形式、實作機器學習演算法之分類結果或其他種結果提供予使用者。

－隱私保護資料發布(privacy preserving data publishing, PPDP)模型：於此模型中，先處理資料，產生新的、去識別化或合成的資料，再提供予使用者。

3.3 資料分析之政策要求事項(選項)

目標：組織若自行、授權或委託第三方進行含有個資之資料(尤其是巨量資料)的分析工作，則隱私政策應包含對資料分析過程保護隱私之承諾及要求。

3.3.1 對外聲明

控制措施：隱私政策應敘明下列項目，並應對外公布適宜之相關內容。

－對資料分析人員，組織僅提供適當程度之經去識別化資料，供其進行資料分析工作。

－組織備妥標準作業程序及完善之控制措施，將資料置於管制環境中，僅供經核准之特定人員進行資料分析。

－組織對資料分析工作之管制及要求。

－組織管控分析產出之流向及存取對象及作法。

－使用分析產出於行銷(或提供服務選項)時，提供當事人表示拒絕之機制。

3.3.2 合法性

控制措施：組織必須能展示其資料分析過程，符合所有適用之法律要求，以及組織之隱私保護政策。

3.3.3 設計時即將隱私遵循納入考量

控制措施：組織實作涉及個資之資料分析過程，應於系統設計階段即將隱私保護納入考量(privacy by design)，而非於後續階段方納入。並應預設系統為隱私保護(privacy by default)。

肆、個資隱私風險管理過程

第 1 部分：隱私保護要求

目標：組織應針對個資處理生命週期相關(蒐集、處理、利用、儲存、傳送、移除)階段，定期執行周延之個資隱私風險管理活動，並發展與其隱私保護有關的風險剖繪。

4.1 個資處理生命週期風險管理過程

控制措施：組織應建立個資處理生命週期各階段之風險管理過程。各階段之風險管理應包含下列子過程：

- 建立全景過程：藉瞭解組織(例：個資處理、職責)、技術環境及影響隱私風險管理之因素(亦即法規因素、契約因素、營運因素與其他因素)達成。
- 風險評鑑過程：藉識別、分析及評估個資隱私原則之風險(可能有負面影響之風險)達成。
- 風險處理過程：藉定義隱私保全要求事項、識別及實作隱私控制措施以避免或減少個資隱私原則之風險達成。
- 溝通及諮詢過程：藉從利益相關者得到資訊、對每一風險管理過程獲得共識，以及通知個資當事人與溝通風險及控制措施達成。
- 監視及審查過程：藉追查風險及控制措施，以及改善過程達成。

4.1.2 涉及個資之系統隱私衝擊評鑑

控制措施：組織應針對涉及個資之系統，定期或發生重大事故後進行隱私衝擊評鑑(PIA)，報告應至少包含下列內容：

- 概述。
- 評鑑範圍。
- 隱私要求事項。
- 風險評鑑(包含識別所有可能之隱私風險及衝擊等級與後果)。
- 風險處理(例：符合法律及法規、最小化資料收集，以避免風險；實作各項資料保護控制措施，以降低風險；經約條款或購買保險，轉移風險)。
- 依據 PIA 結果之結論(敘明剩餘風險及決策)。

4.1.3 依隱私衝擊評鑑實作控制措施

控制措施：組織應依據隱私衝擊評鑑結果，實作個資處理生命週期相關階段之各項控制措施，並定期稽核及審查其有效性。

實作指引：隱私風險係假想之情境，其描述風險源(例：競爭對手通過收買員工)如何能於威脅全景(例：濫用發送電子郵件)中，利用個人資料支援之資產(例：可操作資料之檔案管理系統)，並造成個人資料(例：客戶檔案)發生非所欲事件(例：非法取得個人資料)，因而對個資當事人的隱私產生影響(例：不請自來的募捐、隱私侵犯之感覺等)。

實作指引：風險係以其可能性(likelihood)及後果之嚴重程度(severity)估算。

- 可能性表示發生風險之可能性。此基本上取決於支援之資產面對威脅的脆弱性，以及風險源利用此等脆弱性之能力。
- 後果之嚴重程度表示風險發生後，衝擊的大小。此基本上取決於潛在衝擊之不利影響。

實作指引：風險分析方法通常可分為：定量分析(quantitative analysis)、定性分析(qualitative analysis)及半定量分析(semi-quantitative

analysis)。

- 定量分析：依據確實數值(金額、技術或人為尺度)表示之特定後果，以及風險之發生機率分析風險。此種分析方法通常很複雜，需研究及開發組織特定模型，故一般僅應用於評估最顯著之可能風險。因此種方法通常難以達成期望之精確度，故可使用敏感性分析，測試不同考量之影響。
- 定性分析：使用文字及描述尺度，評鑑所識別風險之相對大小。
- 半定量分析：將描述尺度之點轉換成數值評分(例：〝1〞=罕見、〝5〞=十分肯定會發生；〝1〞=影響極微、〝5〞=影響嚴重)。雖此種方法比定性分析可產生更結構化之風險排序，但不宜依據比較相對風險(即，比較某風險與另一風險之衝擊)產生評分。

實作指引：隱私衝擊評鑑(PIA)通常指對於個資處理之風險識別、風險分析及風險評估的整體過程。隱私衝擊評鑑(PIA)為一項產出，其為風險管理之一部分，隱私衝擊評鑑乃專注於確保遵循隱私權及資料保護法規之要求，以及評鑑於新的或大幅修改計畫或活動中的隱私權含意。

實作指引：隱私衝擊評鑑宜框限於更大範圍之組織風險管理框架內。

實作指引：就資訊安全控制措施而言，需注意並非所有個資處理均要求相同保護等級或型式。組織宜依其面對之特定風險，選取個資處理運作，以協助決定於何種情況下，適合採取何種資訊安全控制措施。風險管理係此過程之核心方法，且隱私控制措施之識別亦宜為組織資訊安全管理框架中不可或缺之一部分。

第 2 部分：個資去識別化過程要求

4.1.4 依隱私衝擊評鑑實作個資去識別化控制措施(選項)

控制措施：組織若進行個資去識別化工作，則應依據對個資去識別化過程之隱私衝擊評鑑結果，實作各項相關控制措施，並定期稽核及審查控制措施之有效性。

4.1.5 依隱私衝擊評鑑實作資料分析控制措施(選項)

控制措施：組織若自行、授權或委託第三方進行涉及個資之(巨量)資料的分析工作，則應依據對資料分析過程之隱私衝擊評鑑(PIA)結果，實作各項相關控制措施，並定期稽核及審查控制措施之有效性。

實作指引：去識別化之程度通常與資料可用性成反比，而隱私風險大小通常與去識別化之程度成正比。組織應依去識別化後之資料用途與可接受之隱私風險大小，決定去識別化之程度，再依資料選擇適當之去識別化作法。

伍、個資保護之隱私原則要求(選項)

本節屬隱私保護要求。所有業者，無論其是否要進行去識別化或使用涉及個資之資料進行分析，若要確認其隱私保護措施是否到位，建議實作符合本節之控制措施。

5.1 同意及選擇原則

目標：組織對個資之蒐集、處理及利用應遵循同意及選擇原則。

5.1.1 同意選擇機制

控制措施：除非個資當事人無不同意之自由，或所適用法律允許無須該當事人同意即可處理個資，否則應向個資當事人提供說明，由當事人選擇是否允許其個資之處理。個資當事人之選擇必須是自由提供、特定及基於充分理解。

5.1.2 選擇加入

控制措施：除非適用之法律允許無須當事人同意下處理敏感之個資，否則應取得個資當事人選擇同意，方可蒐集及處理其敏感個資。

5.1.3 說明選擇及提供加入及退出機制

控制措施：個資當事人得自由選擇是否提供個資時，應向個資當事人解釋給予或不予同意之含義，告知不提供將對其權益之影響。並應提供選擇加入及之後選擇退出之機制。

5.1.4 告知權利

控制措施：於取得個資當事人同意前，應告知其權利，並應向其提供以公開、透明及告知原則所表達之資訊。

5.1.5 未成年人或無行為能力者個資之處理

控制措施：對未成年人或無行為能力者個資之蒐集、處理及利用需取得其監護人同意。

5.1.6 國際傳輸

控制措施：個資之國際傳輸應依法律之規定。

5.1.7 提供個資處置機制

控制措施：應制訂機制，供個資當事人選擇如何處置其個資，及允許個資當事人方便且免費撤回同意。

5.1.8 於蒐集、初次利用或爾後適用時提供行使選擇機制

控制措施：應對個資當事人就有關其個資處理及利用，於蒐集時、初次利用時或爾後適用時，提供清楚、明確、易懂、可取得及可負擔之機制，以便其行使選擇及給予同意。

5.1.9 依法處理個資應儘可能告知當事人

控制措施：無須個資當事人同意，即可依法處理個資時，應儘可能告知個資當事人。當個資當事人有撤回同意之能力並選擇撤回時，除非法律強制，不應為任何目的處理該個資。

5.1.10 後續持有個資告知

控制措施：個資當事人撤回同意後，必要時，組織應告知個資當事人，為遵循法律、法規或契約義務(例：資料持有、可歸責性)，將持有某

些個資之範圍及期限。

5.1.11 及時實作個資取捨

控制措施：組織應依個資當事人於同意(或不同意)選擇所表達之意思，及時實作其取捨。

5.2 目的適法性及特定原則

目標：組織對個資之蒐集、處理及利用應遵循目的適法性及特定原則。

5.2. 1 遵守適用之法律及法規

控制措施：組織應確保蒐集、處理或利用個資之(各)項目的均遵守適用之法律及法規，且未逾越法律及法規。不應處理處理目的不合法之個資。

5.2.2 向個資當事人傳達新目的

控制措施：組織應於為新目的而蒐集、處理或第一次利用個資之前，向個資當事人傳達(各)目的。該陳述應使用清楚且適合當事人之用語。

5.2.3 解釋處理敏感個資之需要

控制措施：適用時，組織應向個資當事人充足解釋處理敏感個資之需要。

5.3 蒐集限制原則

目標：組織對個資之蒐集應堅持蒐集限制原則。

5.3.1 蒐集限制

控制措施：組織應將個資之蒐集限制於適用之法律及法規所允許之特定目的(例如：申辦組織所提供服務)，且嚴格限定於為此目的所必要之範圍內。

5.3.2 不可蒐集非必要個資

控制措施：組織於進行蒐集個資之前，應審慎考量哪些個資係為實現特定目的所必須者，不可蒐集非必要之個資。

5.3.3 記錄所蒐集個資之型式及其理由

控制措施：組織應記錄所蒐集個資之型式及其理由，並納入其資訊處理之政

策及實務作法中。

5.3.4 組織特定之合法目的

控制措施：組織蒐集之個資數量及型式二者均應限制於組織特定之合法目的。

5.3.5 額外資訊蒐集需獲當事人同意

控制措施：組織可能為當事人所請求之特定服務條款外之目的(例：行銷目的)，欲蒐集額外個資。此種額外資訊應僅於獲當事人同意下方得蒐集。

5.3.6 儘可能告知當事人

控制措施：組織可能依適用之法律或法規要求，蒐集某些個資。適當時，應儘可能告知當事人，並應提供當事人是否同意提供此種資訊之選擇。

5.4 資料極小化原則

目標：組織之個資處理程序及其使用之資通訊系統應嚴格遵循資料極小化原則。

5.4.1 揭露對象最小化

控制措施：組織應將處理個資、隱私相關者及個資揭露對象或可存取個資之人員的數目最小化。

5.4.2 僅知原則

控制措施：組織應確保採用〝僅知〞原則，亦即於個資處理之合法目的框架下，應僅對執行正式職務所必要之人員賦予個資存取權限。

5.4.3 降低當事人行為之可觀察性

控制措施：對當事人之互動與交易，應儘可能降低當事人行為之可觀察性並限制所蒐集個資的可連結性。

5.4.4 刪除或廢棄不必要個資

控制措施：一旦個資處理之目的終止，無法定要求保有個資，或是實務上需如此做時，應立即刪除或廢棄個資。

5.5 利用、保留及揭露限制原則

目標：組織應堅持個資之利用、保留及揭露限制原則。

5.5. 1 特定、明確及合法特定目的

控制措施：組織應限制個資之利用、保留及揭露(包括移轉)，為履行特定、明確及合法特定目的所必要者。

5.5.2 特定目的利用

控制措施：除非適用之法律明確要求不同目的之利用，否則應將個資之利用限制於蒐集之前組織所規定之特定目的。

5.5.3 保留期間

控制措施：組織保有個資之時間長度，僅為滿足所陳述特定目的必要的長度，並於之後安全地將其廢棄或匿名化。

5.5.4 特定目的逾期

控制措施：一旦所陳述特定目的逾期，但依適用法律及法規要求留存，組織應鎖住所有個資(亦即將個資歸檔、保全並禁止後續處理及利用)。

5.5.5 網路儲存

控制措施：當個資儲存於組織場域外(例如雲端)時，應依組織法律、法規及與個資當事人之契約要求事項、風險及組織政策，建立保全個資儲存及傳輸安全之技術及管理措施。

實作指引：與雲端供應者簽訂之契約，可要求選擇特定控制措施，亦可規定必須使用特定準則以實作該等控制措施。

5.5.6 網路傳輸

控制措施：當個資需由當事人處經網路傳輸至控制個資之組織，或由控制個資之組織傳輸至個資處理者處時，應使用加密技術，保全個資儲存及傳輸安全。

5.5.7 跨國傳輸

控制措施：當跨國傳輸個資時，組織應知悉所有跨國傳輸之國家或當地額外

特定規定。

5.6 準確性及品質原則

目標：組織應堅持個資之準確性及品質原則。

5.6.1 準確、完整、最新及適度

控制措施：組織應確保所處理之個資為準確、完整、最新(除非有保有過期資料之合法依據)、適度的，且與使用目的相關。

5.6.2 來源可靠性

控制措施：於處理個資前，組織應確保由非個資當事人之來源所蒐集的個資之可靠性。

5.6.3 請求更正補充機制

控制措施：組織應建立個資當事人可請求更正或補充其資料之機制。

5.6.4 驗證當事人聲明有效性及正確性

控制措施：適當時，於變更個資前，組織應使用適當方法驗證個資當事人聲明之有效性及正確性，以確保該等變更經正確授權。

5.6.5 建立確保個資準確性及品質之蒐集程序

控制措施：組織應建立個資蒐集程序，協助確保個資之準確性及品質。

5.6.6 定期核對

控制措施：組織應建立控制機制，以定期核對所蒐集及儲存之個資的準確性及品質。

5.7 公開、透通性及告知原則

目標：組織應堅持個資處理之公開、透通性及告知原則。

5.7.1 告知原則

控制措施：組織應提供個資當事人，關於個資處理之政策、程序及實務作法的清楚且易取得之資訊。告知中應包括：組織名稱、聯絡資訊、處理中之個資、處理目的、處理之邏輯、個資可能揭露對象等。

5.7.2 詳盡告知

控制措施：個資處理目的之描述應足夠詳盡，以使個資當事人瞭解下列事項。

－個資蒐集之特定目的。
－特定目的所要求之個資。
－所規定之處理(包括蒐集、溝通及儲存機制)。
－將獲授權存取個資之人員及個資可能移轉之對象。
－所規定之個資的持有及廢棄要求。

5.7.3 提供當事人選擇

控制措施:組織應揭露提供予個資當事人之選擇及方式,以限制處理、存取、修正及移除其個資。

5.7.4 委外處理

控制措施：若委外處理(包括委外於資料傳輸及蒐集網路中處理)個資，組織應要求及確認受委託者確實於內部記錄及傳達所有影響個資處理之契約義務，並實作相應控制措施。適當時，組織亦應以非機密之程度對外傳達該等契約義務。

5.7.5 重大變更告知

控制措施：當個資處理程序發生重大變更時，組織應告知個資當事人。

5.8 個人參與及存取原則。

目標：組織應堅持個資之個人參與及存取原則。

5.8.1 存取及審查能力

控制措施:組織應給予個資當事人存取及審查其個資之能力，只要其身分先經適當保證等級鑑別，且該存取未被適用之法律禁止。

5.8.2 修訂、更正及移除能力

控制措施:組織應允許個資當事人核對個資之正確性及完整性，並在特定情況下，於適當及可能時修訂、更正或移除其個資。

5.8.3 對揭露對象之要求

控制措施:於知悉對象之情況下，組織應對個資處理者及對資料揭露對象之第三方，提供所有修訂、更正或移除之資訊，並要求採取因應

作為。

5.8.4 簡單、快速及有效率行使權利

控制措施：應建立程序以確保個資當事人能以簡單、快速及有效率之方式行使其權利，且不造成不應有之延誤或成本。

5.8.5 控制存取

控制措施：組織應使用適當之控制措施，以確保個資當事人僅能存取其本身而非其他當事人之個資，除非獲得該當事人授權，代表其存取。

5.9 可歸責性原則

目標：組織對個資之處理應承擔照管職責，並為保護而採用具體與實際的措施。

5.9.1 記錄及溝通所有隱私相關政策、程序及實務

控制措施：於適當時，組織應記錄及向隱私利害相關者溝通所有隱私相關政策、程序及實務作法。

5.9.2 指派專人負責

控制措施：應於組織內指派高階領導階層成員擔任隱私長(chief privacy officer, CPO)負責實作及監督隱私相關政策、程序及實務作法之任務。

5.9.3 傳送個資至第三方

控制措施：當傳送個資至第三方時，應確保第三方接收者一定會經由契約或其他如強制之內部政策(適用之法律及法規可包含關於國際資料移轉之額外要求)等手段，提供相同等級之隱私保護。

5.9.4 認知宣導及教育訓練

控制措施：組織應對可存取個資之人員實施合適的認知宣導及教育訓練。

5.9.5 抱怨處理及糾正程序

控制措施：組織應設立有效率之隱私保護之抱怨處理及糾正程序，供個資當事人使用。

5.9.6 通知所有隱私相關者

控制措施：若發生個資洩露，組織應立即依主管機關之規定及依據風險等級，通知所有相關之隱私相關者，隱私違反事件。

5.9.7 立即通知當事人

控制措施：若發生個資洩露，除非被禁止(如當與執法人員一起工作時)，組織應立即通知當事人關於可能對其造成實質損害之隱私違反，以及採取之解決方法。

5.9.8 建立糾正程序

控制措施:組織應建立糾正程序,就當事人之隱私受侵害,提供相稱之補償。於發生個資洩露時，允許受侵害之個資當事人，取得適當及有效的制裁及/或補救，如矯正、消除或賠償。

5.10 資訊安全原則

目標：組織應堅持個資之資訊安全原則。

5.10.1 確保個資之完整性、機密性及可用性

控制措施：於主管機關許可下，組織應在運作、功能及策略層級上以適宜之控制措施保護個資，以確保個資之完整性、機密性及可用性，並於其整個生命週期中保護其免於受如未經授權之存取、破壞、使用、修改、揭露或損失的風險。

5.10.2 選擇個資處理者

控制措施：組織應確保選擇之個資處理者，對個資處理之關於組織、實體及技術的控制措施提供充分保證，並確保遵循此等控制措施。

5.10.3 建立資安控制措施

控制措施：組織應依據適用之法律及法規要求、安全標準、系統化安全風險評鑑的結果，以及本益分析之結果，建立此等資安控制措施。

5.10.4 相稱之控制措施

控制措施：組織應實作控制措施，相稱於潛在後果之可能性及嚴重性、個資之敏感性、可能受影響之個資當事人數目,以及其被持有之全景。

5.10.5 限制存取

控制措施:組織應對個資之存取,限制於要求存取權限以執行其職責之個人,並限制上述個人之存取僅於其執行其職責所需存取之個資。

5.10.6 因應風險及脆弱性

控制措施：組織應及時解決經由隱私風險評鑑及稽核過程，所發現之風險及脆弱性。

5.10.7 定期審查及重新評鑑

控制措施：於持續之安全風險管理過程中，組織須定期審查及重新評鑑各項相關控制措施之妥善性及有效性。

5.10.8 使用密碼學方式保護直接識別及特定種類個資

控制措施：組織應使用密碼學方式，保護直接識別及特定種類個資，諸如身分證統一編號、護照號碼、健康資料等。並應妥善管理加解密金鑰。

實作指引：資訊安全要求，可參考個資法施行細則第 12 條。

5.11 隱私遵循原則。

目標：組織應堅持隱私遵循原則。

5.11. 1 定期實施稽核

控制措施：組織應使用內部稽核員或受信賴之第三方稽核員，定期實施稽核以查證與證明過程符合資料保護與隱私保全要求事項。

5.11.2 內部控制及獨立監督

控制措施：組織應建立合宜之內部控制措施及獨立之監督機制，確保遵循相關法律，並遵循組織之安全、資料保護與隱私政策與程序。

5.11.3 發展與維護隱私風險評鑑

控制措施：組織應發展與維護隱私風險評鑑，以評估含有個資處理之方案與提供服務者是否遵循資料保護及隱私要求事項。

5.11.4 遵循主管機關要求

控制措施：組織應與主管機關合作並奉行其指引及要求事項。

陸、個資去識別化過程之要求(選項)

本節屬個資去識別化過程要求。擬進行個資去識別化，俾進行資料分析工

作(及據以行銷)之通傳事業組織需符合本節之要求。

6.1 建立有效且周延之個資去識別化過程治理結構

目標：組織應建立有效且周延之個資去識別化過程的治理結構。

6.1.1 人力資源

控制措施：組織應指定足夠數量具技術與法律知識之員工或約用人員進行個資去識別化。並應指定資深員工，負責授權及監督個資去識別化過程。此負責人員應有能力負責個資去識別化主要決策、宣達及協調組織之個資去識別化作法、召集組織內部及外部相關專家，並應能協助高階管理階層決定已去識別化資料之適當揭露形式(亦即公開或有限存取)。

6.1.2 人員訓練

控制措施：組織應經由人員訓練，使個資去識別化工作人員清楚認識個資去識別化技術、所涉及之所有風險及減輕此等風險之措施。尤其是，各工作人員應了解其於確保安全進行去識別化之責任。

6.1.3 獨立及隔離空間及系統

控制措施：若組織於內部進行個資去識別化工作，應提供獨立及隔離(無法連線)空間及系統進行個資去識別化工作，並管制及記錄人員與資料之進出(及存取)，且人員不得攜帶任何具記錄、錄影、照像及通訊功能之工具與設備進入工作區域。工作所需之設備及工具應配置於隔離空間。文具應由管制人員依規定提供，且不得攜出。

6.1.4 判定去識別化之準則

控制措施：組織應備妥經核准之正式程序，敘明判定是否對資料進行個資去識別化及其實施方法，以及產生之資料是否將公開或揭露、公開或揭露原則、揭露對象及揭露方式之準則。

6.1.5 敘明未進行去識別化之原因

控制措施：組織應備妥經核准之正式程序，敘明於實務上個資去識別化可能是有問題或難以達成之情況。例：難以評估重新識別之風險，或是對某些當事人之個資風險太高。

6.1.6 選擇去識別化方法

控制措施：組織應依據法律規定、組織任務、營運要求、資料使用對象及目的、所持有包含個資之資料內容、型式及數量、處理位置、資料揭露對象、揭露方式、揭露範圍及處理成本及風險評鑑結果等因素，選擇適宜之去識別化方法。此等去識別化方法須經組織之高階管理階層核准，且以文件記錄。

6.1.7 全程受監督、留下紀錄

控制措施：資料去識別化過程應留下紀錄、全程受監督(例：全程錄影)，且其紀錄應無法竄改，並定期稽核及不定期抽查紀錄。

6. 2 監督及審查個資去識別化過程之治理安排

目標：組織之高階管理階層應監督及審查個資去識別化過程之治理的安排。

6.2.1 更新個資去識別化知識

控制措施：組織應管理，關於個資去識別化之任何新指引、法規、法律、裁判、行政解釋、可用技術或威脅之相關知識，並據以評估風險。

6.2.2 交流個資去識別化知識

控制措施：組織應與同行業或從事類似工作之其他組織，分享並交流關於個資去識別化之知識。

6.2.3 定期進行隱私衝擊評鑑

控制措施：組織應定期對個資去識別化過程進行隱私衝擊評鑑(PIA)，並應公布其 PIA 報告(之適宜內容)，顯示如何處理風險評鑑過程。PIA 應包含所採用去識別化技術之有效性，以及評估重新識別之風險，以制定風險緩解措施。

6.2.4 決定可接受剩餘風險準則

控制措施：組織應訂定決定已移除個資之資料的可接受剩餘風險之準則。並應由組織之高階管理階層決定已移除個資之資料的可接受剩餘風險。

實作指引：專家用以協助決定資料可識別性風險之原則如下。

原則	解釋	風險值範例
重現性 (Replicability)	根據資料將持續連結至個資當事人之機率，將資料屬性定出風險等級之優先序。	**低**: 病患之口腔疾病，會改變。 **高**: 病患之牙齒照片相對穩定。
資源可用性 (Resource Availability)	判定哪些外部資源含有特定個人之識別資料及資訊中之重覆特徵，以及何人被允許存取該資源。	**低**：實驗室報告中之個人身份通常不會對實驗室外披露。 **高**：個人身份及人口資料往往出現於公共資源中，例：出生、死亡及婚姻狀態。
區別性 (Distinguish)	判定某個資資料可於資料集之中被區別出的程度。	**低**：估計在美國使用出生年、性別及郵遞區號前3碼之組合約有0.04%機率可唯一識別某居民。意指僅經由此等資料之組合可識別特定居民之可能性低。 **高**：估計在美國使用出生日期、性別及5碼郵遞區號可唯一識別某居民之機率超過50%。意指經由此3個資料之組合可識別一半以上的美國人。
評鑑風險(Assess Risk)	必須同時綜合考量重現性、資源可用性及區	**低**：資料不具區別性，但其可能並未獨立重現，且很少

	別性風險。重現性風險、資源可用性風險及區別性風險越高，資料被識別出之風險越高。	於公眾可取用之多個資源中揭露。 **高**：人口資料具高度區別性、高度重現性並揭露於公共資源中。

可使用此等原則，判定資料集之中的個資資料集之風險值。

6.2.5 審查去識別化過程時機

控制措施：組織之高階管理階層應依規劃之期間或發生重大變更時審查去識別化過程。

6.2.6 依回饋分析審查去識別化過程

控制措施：組織應依據對來自利害相關者之回饋的分析，持續且及時審查個資去識別化過程。審查時應使用〝重新識別測試〞技術，評鑑重新識別風險及降低風險之措施。

6.2.7 獨立之系統化檢查

控制措施：組織應對已移除個資之所有資料，進行獨立(非原個資去識別化工作人員)之系統化(自動或人工)檢查。確保其中未包含直接識別資訊，以及非必要保留之間接識別資訊。並確保必要保留之間接識別資訊皆已(經由匿名化、擬匿名化或其他方法)合理去除與個資當事人之連結。

6.3 訂定個資去識別化過程之標準作業程序

目標：組織應訂定個資去識別化過程之標準作業程序，並依此進行個資去識別化工作。

6.3.1 最少處理資料

控制措施：組織應訂定標準作業程序，敘明如何依據處理後之資料用途，對將去識別化之資料集，依隱私原則進行前置處理，僅取出最少需

處理之資料集、內容、欄位或其部分。

6.3.2 依資料型式選擇去識別作法及工具

控制措施：組織應依待移除個資之資料型式(例：書面文字資料、書面圖片、文字檔、資料庫、圖片檔等)，以及不同檔案格式(例：DOC、DOCX、ODF、PDF、PPT、PPTX、TIF、JPG、MPEG、DICOM 等)，選擇適當去識別作法及工具。

6.3.3 建立重新識別威脅模型

控制措施：組織應針對不同資料集，建立對經去識別化資料之重新識別威脅模型，進行隱私衝擊評鑑(PIA)，並依資料用途、釋出對象及方式、資料敏感性，設定可接受之剩餘風險值。可接受之剩餘風險值，應依個別個資當事人、部分個資當事人及所有涉及之個資當事人，分別設定特定值或平均值。各項可接受之剩餘風險值應由高階管理階層核可。

6.3.4 設定推論控制值

控制措施：組織應依資料釋出對象及方式、資料敏感性，設定推論控制之個別群組檻值(例：k-匿名性之最小 k 值、揭露筆數占整體筆數之最小百分比，或是差動隱私法之加雜訊參數值)。不得揭露不符合之資料。

6.3.5 取樣測試

控制措施：若資料集較大，為測試去識別化之效果，可能需先取樣測試。組織應訂定標準取樣程序，先依據信心水準及誤差率決定樣本資料數量，再由來源資料集之中，依隨機方式選取樣本資料。

6.3.6 個資去識別化步驟

控制措施：組織應訂定類似如下之個資去識別化步驟，並依此進行去識別化工作。

步驟 1：由領域專家(即有相關經驗人員)群判定最小可接受使用之資料集，並判定資料集之中各項資料之隱私等級。首先依據去識別化資料之用途，判定最小可接受使用之資料內容、欄位、範圍及數量，並據以判定可能需進行去識別化之資料的最大數量。再判定各項資料屬性(或欄位)係屬直接識別資料、間接識別資料、敏感資料或普通資料等。

步驟 2：將直接識別資料遮蔽(或變換)。即移除直接識別資料或將其匿名

化。

步驟 3：針對不同資料屬性(或欄位)之間接識別與敏感資料，選定對應之去識別化方法。

步驟 4：建立對去識別化後資料之威脅模型。於此步驟中，分析可能使用額外資訊或其他間接識別資料對已去識別化資料進行重新識別攻擊之各種情境，判定各種〝可能威脅〞。

步驟 5：使用步驟 4 所建立之模型，確定重新識別攻擊之風險的檻值。於此步驟中，組織判定使用已去識別化資料之可接受風險，以及可能降低風險之各項控制措施。

步驟 6：由來源資料庫取得(樣本)資料集，進行去識別化測試。若資料量較大，應依控制措施(6.3.5)，由來源資料庫中選取樣本資料。

步驟 7：評估實際之重新識別攻擊風險。即計算實際被重新識別之風險。

步驟 8：比較實際之被重新識別的風險與原設定可接受風險檻值。即比較步驟 7 與步驟 5 之結果。若實際風險值過高，則需考慮使用新的參數或去識別化方式(重複步驟 3 至步驟 8)。

步驟 9：設定去識別化參數並套用至所有需去識別資料。若實際風險值小於最小可接受風險，則套用此等去識別化參數，並對選定資料進行去識別化。

步驟 10：對解決方案進行診斷。測試已去識別資料，以確保其具有足夠效用，並確認於允許之參數範圍內，合理之重新識別攻擊成功之機率小於可接受值。

步驟 11：輸出已去識別資料至外部資料集。於此最後步驟中，輸出已去識別化資料，並將所使用之去識別化技術、參數、威脅模型、風險值及各項相關資料，記錄於書面報告中。

實作指引：個人資料保護法第 2 條第 1 款定義個人資料：指自然人之之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

實作指引：對具有個資之資料去識別化程度通常與資料之可使用程度相反。去識別化程度越高之資料，經常亦會移除越多可供使用之資料。

實作指引：推論控制通常使用之「N 回應 k%支配」規則，指若超過 k%以上之揭露(或公布)資料係來自少於 N 筆資料，則不得揭露(或公布)該等資料。例：不應公布比爾蓋茲所住社區之家庭平均年收入，因其年收入占整個社區之年收入比例太高，若公布此資料，易被用以推估出比爾蓋茲之年收入。

實作指引：個資去識別化技術範例如下：

－修訂或移除個資：使個資成為(人類或電腦)不可視。例：用黑筆將書面資料塗黑、將人臉打馬賽克、移除檔案中個資、將資料加密、移除整筆資料等。

－模糊化個資：於資料中加入隨機〝雜訊〞。例：將某筆個人資料之

年齡加 5 歲，而下 1 筆資料之年齡加 8 歲、只提供對部分資料之統計數字。

－概化個資：降低資料之精確度，使其較不特定。例：將年齡 25 歲，變成年齡 20~29 歲。

－合併個資：將數項個資合併成一資料項，使其較不具敏感性。例：2014 年及格人數為 2 人，2015 年及格人數為 3 人，合併為 2014~2015 年及格人數為 5 人。

－以平均值置換個資：例：將某筆個人資料之年齡以所有資料之平均年齡置換。

－一致性置換個資資料：將所有個資位移相同量，以保持資料間之關係。例：將所有個人資料之年薪均加 10 萬元。

－交換個資資料：將 2 筆資料之個資欄位內容交換。例：將 2 筆資料之年齡交換。

實作指引：控制推論控制之匿名化隱私模型可分成兩大類：*k*-匿名模型及差動隱私模型。

－*k*-匿名模型，旨在使 *k* 匿名化資料集之中的記錄無法對映回原始集中之中的相應記錄，以防止身份揭露。包含 *k*-匿名、*l*-多樣、*t*-閉合等模型。

－差動隱私模型，旨在限制任何個別個資當事人對分析結果之貢獻的影響，進而保護隱私。包含 ε-差動隱私、群眾混合隱私(crowd-blending privacy)、河豚(blowfish)等模型。

實作指引：*k*-匿名性為去識別化後判定是否揭露資料之限制條件。若使用 *k*-匿名性，則組織應僅揭露具相同值筆數大於等於 *k* 之資料。增加 *k* 值可降低資料遭重新識別之風險。可針對不同群組資料，設定不同 *k* 值。*k*-匿名性可與各種去識別化技術一起使用。

6.4 非預期揭露之災難復原計畫

目標：組織應備妥對個資遭非預期揭露之災難復原計畫。

6.4.1 及時因應申述及查詢

控制措施：組織應及時回應來自自認為個人資料遭揭露民眾(或客戶)之申述及查詢，並依已建立之程序採取因應措施。

6.4.2 備妥因應程序

控制措施：組織應備妥程序，因應釋出資料遭重新識別而揭露個人隱私之情況，包含：移除可能揭露個人隱私之資料，重新處理；停止或修

改(採取更嚴格之)去識別化過程。

6.4.3 告知及協助當事人

控制措施：當釋出資料遭重新識別而揭露個人隱私時，組織應告知隱私遭揭露之個人，並協助其採取必要之糾正及彌補措施。

6. 5 揭露資料需定期進行重新識別測試

目標：組織應備妥程序，對已移除個資之揭露資料，依可接受風險，定期進行〝重新識別測試〞。

6.5.1 揭露資料經匿名化或經不可逆之擬匿名處理

控制措施：組織應對釋出及用以進行分析之已去識別化資料，經匿名化或經不可逆之擬匿名處理。

6.5.2 選取測試樣本

控制措施：若資料量巨大，無法對所有已去識別化資料進行〝重新識別測試〞(指於計算能力或經費上不可行)，組織應訂定依據信心水準及誤差率決定樣本資料數，由已去識別化資料中依隨機取樣方式選取測試樣本資料之標準作業程序。若僅測試樣本資料，而非所有資料，將會增加風險，應將此增加之風險納入風險估算。

實作指引：建議於可行時，儘量對所有釋出之去識別化資料進行〝重新識別測試〞。

6.5.3 重新識別測試

控制措施：組織應對擬公開釋出之所有已去識別化資料(或取樣資料)進行〝重新識別測試〞，至少包含下列項目：

－搜尋網頁，嘗試連結個資當事人。

－搜尋全國或地方新聞資料庫，嘗試連結個資當事人。

－搜尋政府單位或其他組織之開放資料，嘗試連結個資當事人。

－以社群網路嘗試連結個資當事人。

6.5.4 定期重新識別測試

控制措施：因公眾可用之資料數量，隨時增長，故組織應定期重新對公開釋出之已去識別化資料進行〝重新識別測試〞，以重新評鑑其風險。若發現其風險超過檻值，組織應立即移除可能揭露個人隱私之資料，重新處理。並停止或修改(採取更嚴格之)去識別化過程。

6.5.5 審核及管制資料流向及使用

控制措施：組織若將已去識別化之資料授權(或委任)特定對象使用，則應備妥標準作業程序，審核及管制資料流向及使用，規定其用途、使用人員資格、使用人數，以及相關軟體、硬體網路及環境管制之要求事項。

6.6 委外處理個資去識別化之要求(選項)

組織若委外處理個資去識別化工作，則適用本要求事項。

目標：委外處理個資去識別化工作時，組織應監督、監視及稽核委外處理活動。

6.6.1 資料攜出需經核准

控制措施：原始資料以不攜出組織場域為原則。含有個資之限制資料複本，應經組織之高階管理階層核准方可攜出場域外。資料複本攜出場域外需滿足最小資料原則。

6.6.2 資料傳送加密及保全

控制措施：含有個資之限制資料複本，實體由組織移轉至受委託單位去識別化場所之過程應以秘密分享方案加密及保全，且過程應全程記錄及錄影。雖不建議，但組織若採取網路傳輸，移轉此等資料至受委託單位時，應使用足夠安全之加密方式，並透過專線或足夠安全之虛擬私有網路(VPN)以秘密分享方案傳送此等資料。

6.6.3 委外契約規定

控制措施：組織應與受委託單位簽定完善之委外契約，敘明受委託單位之相關義務與責任，以及契約終止條件。

6.6.4 禁止進行其他處理及利用

控制措施：組織應監督受委託單位依委託組織契約之要求，對所交付資料進行去識別化工作，不得進行其他處理及利用。

6.6.5 實地稽核及抽查

控制措施：組織應監督受委託單位之去識別化工作，定期實地稽核及不定期無預警抽查。

6.6.6 妥善且安全保存資料

控制措施：若資料複本攜出組織場域，受委託單位須依委託組織之隱私政策及隱私原則，全程妥善且安全保護原始資料及所處理資料。

6.6.7 歸還銷毀所有持有資料

控制措施：受委託單位於完成去識別化工作後，應立即將產出資料及原資料之複本歸還組織，且須確保安全的銷毀所有持有之受委託處理原始資料與產出資料。

6.6.8 定期及不定期重新評估委外工作風險

控制措施：組織應定期及不定期(例：發生重大事件時)，重新評估此項委外工作之風險並控制之。

6.7 對組織資料分析之要求事項(選項)

組織若對含有個資之(巨量)資料進行分析工作，則適用本要求事項。

目標：組織若對含有個資之(巨量)資料進行分析工作，應妥善保護隱私及設計資料分析機制

6.7.1 判定供資料分析合法使用之個資去識別化程度

控制措施：組織應備妥程序，判定供各項資料分析合法使用之個資去識別化程度。而於進行各批資料分析前，對應之去識別化程度，須經高階管理階層核定。且於完成資料去識別化後，須經獨立檢核其妥

善性後，方可用於資料分析。

6.7.2 僅提供經核定去識別化程度之資料

控制措施：僅提供經事先核定去識別化程度之去識別化資料，供獲授權人員進行資料分析。

－應於合法且仍保持其效用之條件下，提供已去識別化之最高聚合程度資料，並盡可能提供最少個資細節。

－應盡可能隱藏資料中之個資及資料間之相互關係。

6.7.3 指定資料分析團隊及負責人

控制措施：組織應指定資料分析團隊及負責人。應經由人員訓練，使團隊成員熟悉資料分析技術、隱私保護觀念、所涉及風險及減輕此等風險之措施。

6.7.4 於管制環境進行資料分析

控制措施：組織應備妥標準作業程序及完善之管制措施，將已適度去識別化資料置於管制環境中，僅供經授權之特定人員進行資料分析工作。

6.7.5 合法及誠信原則

控制措施：對含有個資之資料的分析工作，應符合〝合法及誠信原則〞。合法指對此等資料之分析符合相關法律規定，且若需個資當事人同意，已取得其同意。誠信指已明確且充分告知個資當事人其相關權利(例：可自由選擇撤回同意)。

6.7.6 最少資料使用原則

控制措施：對含有個資之資料的分析工作應符合〝最少資料使用原則〞，意指：

－ 將所涉及之個資數量、隱私利害相關者數目及個資揭露對象或可存取個資之人員數目最小化。

－ 確保採用〝僅知〞原則，亦即於合法分析條件下，僅對執行分析所必要之人員賦予資料取用權限。

－ 一旦資料分析之目的終止，除依法需保存資料，或是實務上

需保存資料，應即時刪除相關資料。保存之資料應加密，安全保存。

6.7.7 預先設定之合法目的

控制措施：組織應嚴格依〝預先設定之合法目的〞進行資料分析工作。確保分析目的均遵從適用之法律，且經高階管理階層預先設定。

6.7.8 透明公開原則

控制措施：組織對含有個資之資料的分析工作應符合〝透明公開原則〞。

－告知個資當事人，關於組織對於分析含有個資之資料的分析工作之政策、程序及實務的清楚且易取得之資訊。

－告知中包括，分析中之資料、分析目的、產出資料可能之應用及揭露對象之型式。

－告知組織提供予個資當事人之選擇及方式，以合法限制或移除分析其資料。

－當資料分析程序發生重大變更時，告知個資當事人。

6.7.9 資訊安全原則

控制措施：對含有個資之資料的分析工作應符合〝資訊安全原則〞。以適宜之控制措施保護含有個資之資料。

6.7.10 可歸責性

控制措施：組織應記錄所有資料分析過程，並實施內部控制與稽核，以達成〝可歸責性〞。

實作指引：為達成可歸責性(accountability)，某些組織會設立資料保護專員，進行內部稽核並處理相關抱怨。

6.7.11 分離分析

控制措施：組織應以分離方式分析不同來源之含有個資的資料，且同一個資當事人之資料應盡可能於不同系統中分析，避免不當連結，識別出個資當事人。

6.7.12 管控分析產出結果流向及存取對象

控制措施：組織若將分析之產出資料授權(或委任)予特定對象使用，則應備

妥標準審核及管理程序，管制產出資料之流向、用途及使用者。

6.7.13 由設計即保護隱私

控制措施：組織實作含有個資之資料的分析過程，應遵循〝由設計即保護隱私(privacy by design, PbD)〞原則。亦即隱私保護遵循宜於系統設計時期即納入考量，而非於後續階段方納入。並將系統預設為隱私保護(privacy by default)。

6.7.14 當事人表達拒絕之處理

控制措施：組織使用資料分析之產出(或已獲當事人同意直接使用其個資)於行銷(或提供服務選項)時，應提供當事人表示拒絕行銷(或服務選項)之管道。於當事人表達拒絕接受行銷(或服務選項)時，應立即停止對其行銷(或服務選項)，並周知所屬人員，或採行防範所屬人員再次行銷(或服務選項)之措施。

柒、重新識別個資之要求(選項)

本節屬個資去識別化過程之要求。擬進行個資去識別化，俾進行資料分析工作(及據以行銷)之通傳事業組織，必須重新識別已去識別化資料中之個資時，需符合本節之要求。

重新識別係將已去識別化資料與個資當事人重新建立連結之過程。此將增加去識別化過程之複雜度。組織需重新識別個資當事人之理由可能包括：

－法律或法規要求。

－進行符合性稽核。

－重大發現需通知個資當事人或相關單位。

－對資料完整性之檢驗。

－檢查是否有疑似重複之資料。

－加入新資料。

－連結至額外研究變量。

－進行後續進一步研究。

本節內容係依據 CNS 29191 標準之所有要求事項。

7.1 僅可查證資料屬性真實性

目標：經匿名(或擬匿名)處理後資料之接收者應僅能鑑別個資當事人之資料屬性，而無法識別出個資當事人。

7.1.1 僅可查證但無法識別當事人

控制措施：經匿名(或擬匿名)處理後之資料，不得提供任何可用以識別出個資當事人之資料，但必要時可允許資料接收者查證經匿名(或擬匿名)處理後之資料(或其屬性)是否真實。

7.2 聚合後無法連結

目標：同一個資當事人之經匿名(或擬匿名)處理後之不同資料，不得提供具有聚合後能連結至該個資當事人之資訊。

7.2.1 聚合後不含可連結當事人資料

控制措施：資料接收者取得之經匿名(或擬匿名)處理資料，不得包含可據以連結個資當事人之間接識別資料。

7.3 重新識別當事人之能力

目標：資料經可逆之擬匿名處理後，應可由個資控制者重新識別個資當事人。

7.3.1 秘密分享管制擬匿名法

控制措施：組織若需採之擬匿名法進行個資去識別化，應使用加密法及秘密分享機制管制重新識別所需資訊。

7.3.2 備有重新識別個資合法程序

控制措施：必要時，組織應備有重新識別個資之合法程序，規定啟動時機、所使用方法、所需資訊、授權及啟動重新識別之流程。並依此啟動重新識別程序。對不同對象揭露個資時，宜使用不同擬匿名化函數或相同函數不同參數。

7.3.3 定期審查程序之有效性

控制措施：組織應定期審查合法重新識別個資之程序的有效性。

7.3.4 能重新識別當事人

控制措施：為使個資控制者之後能重新識別個資當事人，將資料經可逆之擬匿名處理後產生之紀錄單及重新識別所需之必要資料，應提供足以重新識別個資當事人之必要資訊。

7.3.5 妥善加密持續保存紀錄單

控制措施：組織對將個資資料經可逆之擬匿名處理所產生之紀錄單及重新識別所需之必要資料，應妥善加密，持續保存。

實作指引：於適當情況下，組織可使用其他資訊以重新識別個資當事人。

7.4 提供正確重新識別之證據

目標：於合法且有必要情況下(例如：法定之稽核)，組織應提供能正確重新識別個資當事人之證據。

7.4.1 提供正確履行重新識別個資當事人之程序的證據

控制措施：為避免不誠實宣稱，組織應提供正確履行重新識別個資當事人之程序的證據。

7.4.2 記錄重新識別過程

控制措施：組織於合法且有必要情況下，重新識別個資當事人資料之過程應留下紀錄、全程受監督(例：全程錄影)，且其紀錄應無法竄改。

參考資料

(1)法規

個人資料保護法，法務部

個人資料保護法施行細則，法務部

電信事業資訊安全管理要點，國家通訊傳播委員會

國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法，國家通訊傳播委員會

法務部，法律字第 10303513040 號函

(2)標準

CNS 27001 資訊技術－安全技術－資訊安全管理系統－要求事項

CNS 29100 資訊技術-安全技術-隱私權框架

CNS 29191 資訊技術-安全技術-部分匿名及部分去連結鑑別之要求事項

CNS 27018 資訊技術－安全技術－公用雲 PII 處理者保護個人可識別資訊(PII)之作業規範

ISO/IEC 29101:2013 Information technology -- Security techniques -- Privacy architecture framework.

ISO/IEC 29134:2017 Information technology – Security techniques – Guidelines for privacy impact assessment.

ISO/IEC 29151:2017 Information technology — Security techniques — Code of practice for personally identifiable information protection.

(3)其他出版品

Simson L. Garfinkel, *De-Identification of Personal Informatio*n, NISTIR 8053, 2015. *http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf*

*Anonymisation: managing data protection risk code of practic*e, ICO, UK, 2012.

https://ico.org.uk/media/1061/anonymisation-code.pdf

IHE IT Infrastructure Technical Committee, *IHE IT Infrastructure Handbook: De-Identification*, 2014.

Bradley Malin, *A De-identification Strategy Used for Sharing One Data Provider's Oncology Trials Data through the Project Data Sphere® Repository*, 2013.

Giuseppe D' Acquisto, Josep Domingo-Ferrer, Panayiotis Kikiras, Vicenç Torra, Yves-Alexandre de Montjoye, Athena Bourka,*Privacy by design in big data-An overview of privacy enhancing technologies in the era of big data analytics*, European Union Agency For Network And Information Security, 2015.

附件 1

通傳事業個人資料去識別化過程驗證技術規範自評表

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
參、隱私權政策			
<u>要求事項</u> **<u>3.1</u>**	組織之高階管理階層，應依營運要求及相關法律與法規，建立隱私政策，提供隱私保護之管理指導方針及支持。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **3.1.1** **隱私政策要求事項**	隱私權政策應如下： －符合相關法律與法規要求及組織之營運要求。 －敘明組織之高階管理階層對隱私權保護之管理指導方針及支持。 －敘明組織蒐集、處理、儲存、利用、刪除及銷毀個人資料之適法性及及相關措施。 －界定組織蒐集、處理、儲存及利用個人資料之範圍。 －敘明組織對含有個資之資料的存取管控，以及使用紀錄、軌跡資料及證據保存、稽核之規定與機制。 －敘明含有個資之資料，保存之格式、方法、期限及相關保護措施，以及保有個資之特定目的消失或期限屆滿時之處置。 －敘明組織之隱私權利害相關者。 －提供下列事項之框架，並設定目標： ● 管審會之組成、職掌及召開時機。 ● 各工作小組之組成及任務。 ● 認知宣導及教育訓練要求。 ● 隱私權保護之稽核要求。		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
	● 對系統實施隱私衝擊評鑑之要求。 －敘明隱私權事宜之通報及應變機制。 －敘明委外處理含有個資之資料的契約要求及對委外廠商之稽核要求。 －敘明對隱私權政策持續改善之承諾。 －使各隱私權利害相關者可適時且容易取得。		
控制措施 3. 1.2 書面載明隱私政策並傳達	組織應以書面載明其隱私權政策，並有效及適時傳達予隱私利害相關者。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 3.1.3 隱私政策審查時機	隱私政策應依規劃之期間或發生重大變更時審查，以確保其持續的合宜性、適切性及有效性。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 3.1.4 依隱私利害相關者補充規定	隱私政策應依不同隱私利害相關者，補充規定對應之詳細個資處理規則及義務。(例：針對接觸或利用個資之各特定部門或員工，訂定對應之管控程序。)		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
控制措施 3.1.5 實作程序、存取控制、告知條款、稽核要求	隱私權政策應敘明設置哪些用以實作符合隱私權政策之程序、存取控制、告知條款、稽核要求等。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 3.1.6 內部隱私政策	對內之隱私權政策應載明組織採用之隱私保護目標、規則、義務、懲處規定、限制及/或控制措施，以滿足與組織個資處理生命週期各階段相關之隱私保全要求事項。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 3.1.7 外部隱私政策	組織應傳達予外部隱私權利害相關者下列資訊： －組織之名稱及辦公室地址，以及個資當事人可取得額外資訊之連絡窗口。 －所有相關之個資處理者的名稱。 －將蒐集之個資類別。 －蒐集個資之特定目的及適法性。 －個資利用之期間、領域、對象及方式。 －關於移轉個資至個資處理者之作法。 －個資保護之實務作法聲明及其目的。 －個資當事人得自由選擇提供個人資料時，不提供將對其權益之影響，以及選擇加入及之後		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
	選擇退出之機制。 －個資當事人對其被蒐集之個資的法律權利。 －提供個資當事人行使權利之機制，包含： ● 依當事人之請求，就蒐集之個人資料，答覆查詢、提供閱覽或製給複製本之機制。 ● 依當事人之請求，更正或補充資料之機制。		
控制措施 3.1.8 違反隱私管理後果認知	組織應備妥措施，使相關人員(尤其是個資處理者)認知違反隱私政策或安全要求之可能後果，包括： －對個資處理者 ● 委外處理者：法律責任、賠償、業務喪失、品牌或聲譽之損害等。 ● 內部處理者：懲處、賠償等。 －對員工及約用人員：懲處、賠償等。 －對個資當事人：造成身體、物質、隱私及情緒等傷害。 組織並應建立正式程序，以因應違反隱私政策之行動。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 3.1.9 認知宣導及教育訓練	組織應每年定期對蒐集、處理或利用含有個資之資料的所有員工、約用人員、委外廠商人員及隱私權利害相關者進行認知宣導及教育訓練。		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
控制措施 3.1.10 定期內部稽核	組織應每年定期實施隱私保護、個資去識別化及涉及個資之資料分析的內部稽核。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 3.1.11 委外處理含有個資之資料	組織若委外處理含有個資之資料，則委外處理廠商應遵循組織之隱私政策及要求事項。委外處理廠商應依據組織之隱私政策及要求事項，訂定相對應之隱私保護制度與控制措施。組職並應監督並定期及不定期稽核委外處理廠商之作業。組職應訂定資料移轉及於資料處理完畢後歸還及移除資料之作業程序，並監督廠商遵循。		☐符合 ☐不符合 ☐部分符合 ☐不適用
<u>要求事項 3.2</u>	**(個資去識別化之政策要求事項)** **組織若進行個資去識別化，則隱私政策應包含對去識別化過程保護隱私之承諾及要求。**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 3.2.1 對外聲明	組織若進行個資去識別化過程，隱私政策應包含下列項目，並應對外公布適宜之相關內容。 －敘明組織之去識別化作法，並以一般用語描述將使用哪些去識別化技術及其產出。 －敘明經去識別化資料之可能重新識別風險，以及組織決定接受風險之原則。 －敘明去識別化資料之釋出原則。包含何種資料會公開、何種資料會對哪些特定對象有限揭露、或何種資料會供組織或他方利用，並敘明對應之相		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
	關風險、如何衡量與取捨、考量或未考量哪些因素、原因為何。		
控制措施 3.2.2 選擇適宜去識別化作法	組織應依含有個資之資料的敏感性，針對不同資料釋出對象、應用及環境，規定適宜之〝隱私保護之私密資訊使用模型〞，並選擇適宜之去識別化作法。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 3.2.3 重新識別測試及風險評鑑	組織於利用、開放、揭露或移轉經去識別化資料前，應對資料進行〝重新識別測試〞及風險評鑑。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 3.2.4 資料揭露控制	組織若對公眾公開或對特定對象揭露經去識別化資料，應告知資料開放或揭露對象，使用此等資料之相關義務、責任、限制及風險，以及不當使用或移轉此等資料應負之責任及可能後果。並應要求資料揭露對象簽署資料使用切結書。		☐符合 ☐不符合 ☐部分符合 ☐不適用
<u>要求事項 3.3</u>	**(資料分析之要求事項)** **組織若自行、授權或委託第三方進行含有個資之資料(尤其是巨量資料)的分析工作，則隱私權政策應包含對資料分析過程保護隱私之承諾及要求。**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 3.3.1 對外聲明	隱私權政策應敘明下列項目，並應對外公布適宜之相關內容。 －對資料分析人員，組織僅提供適當程度之經去識別化資料，供其進行資料分析工作。 －組織備妥標準作業程序及完		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
	善之控制措施，將資料置於管制環境中，僅供經核准之特定人員進行資料分析。 －組織對資料分析工作之管制及要求。 －組織管控分析產出之流向及存取對象及作法。 －使用分析產出於行銷(或提供服務選項)時，提供當事人表示拒絕之機制。		
控制措施 3.3.2 合法性	組織必須能展示其資料分析過程，符合所有適用之法律要求，以及組織之隱私保護政策。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 3.3.3 設計時即將隱私遵循納入考量	組織實作含有個資之資料分析過程，應於系統設計階段即將隱私保護納入考量(privacy by design)，而非於後續階段方納入。並應預設系統為隱私保護(privacy by default)。		☐符合 ☐不符合 ☐部分符合 ☐不適用
肆、個資隱私風險管理過程			
<u>要求事項 4.1</u>	**組織應針對個資處理生命週期相關(蒐集、處理、利用、儲存、傳送、移除)階段，定期執行周延之個資隱私風險管理活動，並發展與其隱私保護有關的風險剖繪。**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 4.1.1 個資處理生命週期風	組織應建立個資處理生命週期各階段之風險管理過程。各階段之風險管理應包含下列子過程： －建立全景過程：藉瞭解組織(例：個資處理、職責)、技術環境及影響隱私風險管理之		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
險管理過程	因素(亦即法規因素、契約因素、營運因素與其他因素)達成。 －風險評鑑過程：藉識別、分析及評估個資隱私原則之風險(可能有負面影響之風險)達成。 －風險處理過程：藉定義隱私保全要求事項、識別及實作隱私控制措施以避免或減少個資隱私原則之風險達成。 －溝通及諮詢過程：藉從利益相關者得到資訊、對每一風險管理過程獲得共識，以及通知個資當事人與溝通風險及控制措施達成。 －監視及審查過程：藉追查風險及控制措施，以及改善過程達成。		
控制措施 **4.1.2** 涉及個資之系統隱私衝擊評鑑	組織應針對涉及個資之系統，定期或發生重大事故後進行隱私衝擊評鑑(PIA)，報告應至少包含下列內容： －概述。 －評鑑範圍。 －隱私要求事項。 －風險評鑑(包含識別所有可能之隱私風險及衝擊等級與後果)。 －風險處理(例：符合法律及法規、最小化資料收集，以避免風險；實作各項資料保護控制措施，以降低風險；經約條款		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
	或購買保險，轉移風險)。 －依據 PIA 結果之結論(敘明剩餘風險及決策)。		
控制措施 4.1.3 依隱私衝擊評鑑實作控制措施	組織應依據隱私衝擊評鑑結果，實作個資處理生命週期相關階段之各項控制措施，並定期稽核及審查其有效性。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 4.1.4 依隱私衝擊評鑑實作個資去識別化控制措施	組織若進行個資去識別化工作，則應依據對個資去識別化過程之隱私衝擊評鑑結果，實作各項相關控制措施，並定期稽核及審查控制措施之有效性。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 4.1.5 依隱私衝擊評鑑實作資料分析控制措施	組織若自行、授權或委託第三方進行含有個資之(巨量)資料的分析工作，則應依據對資料分析過程之隱私衝擊評鑑結果，實作各項相關控制措施，並定期稽核及審查控制措施之有效性。		☐符合 ☐不符合 ☐部分符合 ☐不適用

伍、個人可識別資訊(個資)之隱私權原則要求

(一)同意及選擇原則			
項目	**控制措施**	**文件名稱、章節出處或紀錄名稱**	**自評結果**
<u>要求事項</u> **<u>5.1</u>**	組織對個資之蒐集、處理及利用應遵循同意及選擇原則。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **5.1.1** 同意選擇機制	除非個資當事人無不同意之自由，或所適用法律允許無須該當事人同意即可處理個資，否則應向個資當事人提供說明，由當事人選擇是否允許其個資之處理。個資當事人之選擇必須是自由提供、特定及基於充分理解。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **5.1.2** 選擇加入	除非適用之法律允許無須當事人同意下處理敏感之個資，否則應取得個資當事人選擇同意，方可蒐集及處理其敏感個資。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **5.1.3** 說明選擇及提供加入及退出機制	個資當事人得自由選擇是否提供個資時，應向個資當事人解釋給予或不予同意之含義，告知不提供將對其權益之影響。並應提供選擇加入及之後選擇退出之機制。。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **5.1.4** 告知權利	於取得個資當事人同意前，應告知其權利，並應向其提供以公開、透明及告知原則所表達之資訊。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **5.1.5** 未成年	對未成年人或無行為能力者個資之蒐集、處理及利用需取得其監護人同意。		☐符合 ☐不符合 ☐部分符合 ☐不適用

人或無行為能力者個資之處理			
控制措施 5.1.6 國際傳輸	個資之國際傳輸應依法律之規定。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.1.7 提供個資處置機制	應制訂機制，供個資當事人選擇如何處置其個資，及允許個資當事人方便且免費撤回同意。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.1.8 於蒐集、初次利用或爾後適用時提供行使選擇機制	應對個資當事人就有關其個資處理及利用，於蒐集時、初次利用時或爾後適用時，提供清楚、明確、易懂、可取得及可負擔之機制，以便其行使選擇及給予同意。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.1.9 依法處理個資應儘可能告知當事人	無須個資當事人同意，即可依法處理個資時，應儘可能告知個資當事人。當個資當事人有撤回同意之能力並選擇撤回時，除非法律強制，不應為任何目的處理該個資。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 5.1.10 後續持有個資告知	個資當事人撤回同意後，必要時，組織應告知個資當事人，為遵循法律、法規或契約義務(例：資料持有、可歸責性)，將持有某些個資之範圍及期限。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.1.11 及時實作個資取捨	組織應依個資當事人於同意(或不同意)選擇所表達之意思，及時實作其取捨。		☐符合 ☐不符合 ☐部分符合 ☐不適用
(二)目的適法性及規定原則			
項目	**控制措施**	**文件名稱、章節出處或紀錄名稱**	**自評結果**
<u>要求事項 5.2</u>	**組織對個資之蒐集、處理及利用應堅持目的適法性及規定原則。**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.2. 1 遵守適用之法律及法規	組織應確保蒐集、處理或利用個資之(各)項目的均遵守適用之法律及法規，且未逾越法律及法規。不應處理處理目的不合法之個資。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.2.2 向個資當事人傳達新目的	組織應於為新目的而蒐集、處理或第一次利用個資之前，向個資當事人傳達(各)目的。該陳述應使用清楚且適合當事人之用語。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.2.3	適用時，組織應向個資當事人充足解釋處理敏感個資之需要。		☐符合 ☐不符合

解釋處理敏感個資之需要			☐部分符合 ☐不適用
(三)蒐集限制原則			
項目	**控制措施**	**文件名稱、章節出處或紀錄名稱**	**自評結果**
<u>要求事項 5.3</u>	**組織對個資之蒐集應堅持蒐集限制原則。**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.3.1 蒐集限制	組織應將個資之蒐集限制於適用之法律及法規所允許之特定目的(例如：申辦組織所提供服務)，且嚴格限定於為此目的所必要之範圍內。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.3.2 不可蒐集非必要個資	組織於進行蒐集個資之前，應審慎考量哪些個資係為實現特定目的所必須者，不可蒐集非必要之個資。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.3.3 記錄所蒐集個資之型式及其理由	組織應記錄所蒐集個資之型式及其理由，並納入其資訊處理之政策及實務作法中。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.3.4 組織特定之合法目的	組織蒐集之個資數量及型式二者均應限制於組織特定之合法目的。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 5.3.5 額外資訊蒐集需獲當事人同意	組織可能為當事人所請求之特定服務條款外之目的(例：行銷目的)，欲蒐集額外個資。此種額外資訊應僅於獲當事人同意下方得蒐集。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.3.6 儘可能告知當事人	組織可能依適用之法律或法規要求，蒐集某些個資。適當時，應儘可能告知當事人，並應提供當事人是否同意提供此種資訊之選擇。		☐符合 ☐不符合 ☐部分符合 ☐不適用
(四)資料極小化原則			
項目	**控制措施**	**文件名稱、章節出處或紀錄名稱**	**自評結果**
<u>要求事項 5.4</u>	**組織之個資處理程序及其使用之資通訊系統應嚴格遵循資料極小化原則。**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.4.1 揭露對象最小化	組織應將處理個資、隱私權相關者及個資揭露對象或可存取個資之人員的數目最小化。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.4.2 僅知原則	組織應確保採用〝僅知〞原則，亦即於個資處理之合法目的框架下，應僅對執行正式職務所必要之人員賦予個資存取權限。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.4.3	對當事人之互動與交易，應儘可能降低當事人行為之可觀察性並限制所蒐集個資的可連結性。		☐符合 ☐不符合 ☐部分符合

降低當事人行為之可觀察性			☐不適用
控制措施 **5.4.4** 刪除或廢棄不必要個資	一旦個資處理之目的終止，無法定要求保有個資，或是實務上需如此做時，應立即刪除或廢棄個資。		☐符合 ☐不符合 ☐部分符合 ☐不適用
(五)利用、保留及揭露限制原則			
項目	**控制措施**	**文件名稱、章節出處或紀錄名稱**	**自評結果**
<u>要求事項 5.5</u>	**組織應堅持個資之利用、保留及揭露限制原則。**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **5.5. 1** 特定、明確及合法特定目的	組織應限制個資之利用、保留及揭露(包括移轉)於，為履行特定、明確及合法特定目的所必要者。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **5.5.2** 特定目的利用	除非適用之法律明確要求不同目的之利用，否則應將個資之利用限制於蒐集之前組織所規定之特定目的。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **5.5.3** 保留期間	組織保有個資之時間長度，僅為滿足所陳述特定目的必要的長度，並於之後安全地將其廢棄或匿名化。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 5.5.4 特定目的逾期	一旦所陳述特定目的逾期，但依適用法律及法規要求留存，組織應鎖住所有個資(亦即將個資歸檔、保全並禁止後續處理及利用)。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.5.5 網路儲存	當個資儲存於組織場域外(例如雲端)時，應依組織法律、法規及與個資當事人之契約要求事項、風險及組織政策，建立保全個資儲存及傳輸安全之技術及管理措施。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.5.6 網路傳輸	當個資需由當事人處經網路傳輸至控制個資之組織，或由控制個資之組織傳輸至個資處理者處時，應使用加密技術，保全個資儲存及傳輸安全。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.5.7 跨國傳輸	當跨國傳輸個資時，組織應知悉所有跨國傳輸之國家或當地額外特定規定。		☐符合 ☐不符合 ☐部分符合 ☐不適用
(六)準確性及品質原則			
項目	**控制措施**	**文件名稱、章節出處或紀錄名稱**	**自評結果**
<u>要求事項 5.6</u>	**組織應堅持個資之準確性及品質原則。**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.6.1 準確、完整、最新及適度	組織應確保所處理之個資為準確、完整、最新(除非有保有過期資料之合法依據)、適度的，且與使用目的相關。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 5.6.2 來源可靠性	於處理個資前，組織應確保由非個資當事人之來源所蒐集的個資之可靠性。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.6.3 請求更正補充機制	組織應建立個資當事人可請求更正或補充其資料之機制。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.6.4 驗證當事人聲明有效性及正確性	適當時，於變更個資前，組織應使用適當方法驗證個資當事人聲明之有效性及正確性，以確保該等變更經正確授權。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.6.5 建立確保個資準確性及品質之蒐集程序	組織應建立個資蒐集程序，協助確保個資之準確性及品質。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.6.6 定期核對	組織應建立控制機制，以定期核對所蒐集及儲存之個資的準確性及品質。		☐符合 ☐不符合 ☐部分符合 ☐不適用

(七)公開、透通性及告知原則			
項目	**控制措施**	**文件名稱、章節出處或紀錄名稱**	**自評結果**
<u>要求事項</u> **<u>5.7</u>**	**應堅持個資處理之公開、透通性及告知原則。**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **5.7.1** 告知原則	組織應提供個資當事人，關於個資處理之政策、程序及實務作法的清楚且易取得之資訊。告知中應包括：組織名稱、聯絡資訊、處理中之個資、處理目的、處理之邏輯、個資可能揭露對象等。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **5.7.2** 詳盡告知	個資處理目的之描述應足夠詳盡，以使個資當事人瞭解下列事項。 －個資蒐集之特定目的。 －特定目的所要求之個資。 －所規定之處理(包括蒐集、溝通及儲存機制)。 －將獲授權存取個資之人員及個資可能移轉之對象。 －所規定之個資的持有及廢棄要求。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **5.7.3** 提供當事人選擇	組織應揭露提供予個資當事人之選擇及方式，以限制處理、存取、修正及移除其個資。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **5.7.4** 委外處理	若委外處理(包括委外於資料傳輸及蒐集網路中處理)個資，組織應要求及確認受委託者確實於內部記錄及傳達所有影響個資處理之契約義務，並實作相應控制措施。適當時，組織亦應以非機密之程度對外傳達該等契約義務。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 5.7.5 重大變更告知	當個資處理程序發生重大變更時，組織應告知個資當事人。		☐符合 ☐不符合 ☐部分符合 ☐不適用
(八)個人參與及存取原則			
項目	**控制措施**	**文件名稱、章節出處或紀錄名稱**	**自評結果**
<u>要求事項 5.8</u>	**組織應堅持個資之個人參與及存取原則。**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.8. 1 存取及審查能力	組織應給予個資當事人存取及審查其個資之能力，只要其身分先經適當保證等級鑑別，且該存取未被適用之法律禁止。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.8.2 修訂、更正及移除能力	組織應允許個資當事人核對個資之正確性及完整性，並在特定情況下，於適當及可能時修訂、更正或移除其個資。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.8.3 對揭露對象之要求	於知悉對象之情況下，組織應對個資處理者及對資料揭露對象之第三方，提供所有修訂、更正或移除之資訊，並要求採取因應作為。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.8. 4 簡單、快速及有	應建立程序以確保個資當事人能以簡單、快速及有效率之方式行使其權利，且不造成不應有之延誤或成本。		☐符合 ☐不符合 ☐部分符合 ☐不適用

效率行使權利			
控制措施 5.8.5 控制存取	組織應使用適當之控制措施，以確保個資當事人僅能存取其本身而非其他當事人之個資，除非獲得該當事人授權，代表其存取。		☐符合 ☐不符合 ☐部分符合 ☐不適用
(九)可歸責性原則			
項目	**控制措施**	**文件名稱、章節出處或紀錄名稱**	**自評結果**
<u>要求事項 5.9</u>	組織對個資之處理應承擔照管職責並為保護而採用具體與實際的措施。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.9.1 記錄及溝通所有隱私相關政策、程序及實務	於適當時，組織應記錄及向隱私利害相關者溝通所有隱私相關政策、程序及實務作法。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.9.2 指派專人負責	應於組織內指派高階領導階層成員擔任隱私長(chief privacy officer, CPO)負責實作及監督隱私相關政策、程序及實務作法之任務。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.9.3 傳送個資至第三方	當傳送個資至第三方時，應確保第三方接收者一定會經由契約或其他如強制之內部政策(適用之法律及法規可包含關於國際資料移轉之額外要求)等手段，提供相同等級之隱私保護。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措	組織應對可存取個資之人員實施		☐符合

施 **5.9.4** 認知宣導及教育訓練	合適的認知宣導及教育訓練。		☐不符合 ☐部分符合 ☐不適用
控制措施 **5.9.5** 抱怨處理及糾正程序	組織應設立有效率之抱怨處理及糾正程序，供個資當事人使用。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **5.9.6** 通知所有隱私相關者	若發生個資洩露，組織應立即依主管機關之規定及依據風險等級，通知所有相關之隱私相關者，隱私違反事件。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **5.9.7** 立即通知當事人	若發生個資洩露，除非被禁止(如當與執法人員一起工作時)，組織應立即通知當事人關於可能對其造成實質損害之隱私權違反，以及採取之解決方法。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **5.9.8** 建立糾正程序	組織應建立糾正程序，就當事人之隱私受侵害，提供相稱之補償。於發生個資洩露時，允許受侵害之個資當事人，取得適當及有效的制裁及/或補救，如矯正、消除或賠償。		☐符合 ☐不符合 ☐部分符合 ☐不適用
(十)資訊安全原則			
項目	**控制措施**	**文件名稱、章節出處或紀錄名稱**	**自評結果**
<u>要求事項</u> **<u>5.10</u>**	**組織應堅持個資之資訊安全原則。**		☐符合 ☐不符合 ☐部分符合

			☐不適用
控制措施 5.10.1 確保個資之完整性、機密性及可用性	於主管機關許可下，組織應在運作、功能及策略層級上以適宜之控制措施保護個資，以確保個資之完整性、機密性及可用性，並於其整個生命週期中保護其免於受如未經授權之存取、破壞、使用、修改、揭露或損失的風險。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.10.2 選擇個資處理者	組織應確保選擇之個資處理者，對個資處理之關於組織、實體及技術的控制措施提供充分保證，並確保遵循此等控制措施。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.10.3 建立資安控制措施	組織應依據適用之法律及法規要求、安全標準、系統化安全風險評鑑的結果，以及本益分析之結果，建立此等資安控制措施。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.10.4 相稱之控制措施	組織應實作控制措施，相稱於潛在後果之可能性及嚴重性、個資之敏感性、可能受影響之個資當事人數目，以及其被持有之全景。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.10.5 限制存取	組織應對個資之存取，限制於要求存取權限以執行其職責之個人，並限制上述個人之存取僅於其執行其職責所需存取之個資。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.10.6	組織應及時解決經由隱私風險評鑑及稽核過程，所發現之風險及脆弱性。		☐符合 ☐不符合 ☐部分符合

因應風險及脆弱性			☐不適用
控制措施 5.10.7 定期審查及重新評鑑	於持續之安全風險管理過程中，組織須定期審查及重新評鑑各項相關控制措施之妥善性及有效性。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.10.8 使用密碼學方式保護直接識別及特定種類個資	組織應使用密碼學方式，保護直接識別及特定種類個資，諸如身分證統一編號、護照號碼、健康資料等。並應妥善管理加解密金鑰。		☐符合 ☐不符合 ☐部分符合 ☐不適用
(十一) 隱私遵循原則			
項目	**控制措施**	**文件名稱、章節出處或紀錄名稱**	**自評結果**
<u>要求事項 5.11</u>	**組織應堅持隱私遵循原則。**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.11.1 定期實施稽核	組織應使用內部稽核員或受信賴之第三方稽核員，定期實施稽核以查證與證明過程符合資料保護與隱私保全要求事項。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.11.2 內部控	組織應建立合宜之內部控制措施及獨立之監督機制，確保遵循相關法律，並遵循組織之安全、資料保護與隱私權政策與程序。		☐符合 ☐不符合 ☐部分符合 ☐不適用

制及獨立監督			
控制措施 5.11.3 發展與維護隱私風險評鑑	組織應發展與維護隱私風險評鑑，以評估含有個資處理之方案與提供服務者是否遵循資料保護及隱私要求事項。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 5.11.4 遵循主管機關要求	組織應與主管機關合作並奉行其指引及要求事項。		☐符合 ☐不符合 ☐部分符合 ☐不適用

陸、個資去識別化過程之要求

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
<u>要求事項 6.1</u>	**組織應建立有效且周延之個資去識別化過程的治理結構**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.1.1 遵循主管機關要求	組織應指定足夠數量具技術與法律知識之員工或約用人員進行個資去識別化。並應指定資深員工，負責授權及監督個資去識別化過程。 此負責人員應有能力負責個資去識別化主要決策、宣達及協調組織之個資去識別化作法、召集組織內部及外部相關專家，並應能協助高階管理階層決定已去識別化資料之適當揭露形式(亦即公開或有限存取)。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.1.2 人員訓練	組織應經由人員訓練，使個資去識別化工作人員清楚認識個資去識別化技術、所涉及之所有風險及減輕此等風險之措施。尤其是，各工作人員應了解其於確保安全進行去識別化之責任。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 6.1.3 獨立及隔離空間及系統	若組織於內部進行個資去識別化工作，應提供獨立及隔離(無法連線)空間及系統進行個資去識別化工作，並管制及記錄人員與資料之進出(及存取)，且人員不得攜帶任何具記錄、錄影、照像及通訊功能之工具與設備進入工作區域。工作所需之設備及工具應配置於隔離空間。文具應由管制人員依規定提供，且不得攜出。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.1.4 判定去識別化之準則	組織應備妥經核准之正式程序，敘明判定是否對資料進行個資去識別化及其實施方法，以及產生之資料是否將公開或揭露、公開或揭露原則、揭露對象及揭露方式之準則。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.1.5 未進行去識別化之原因	組織應備妥經核准之正式程序，敘明於實務上個資去識別化可能是有問題或難以達成之情況。例：難以評估重新識別之風險，或是對某些當事人之個資風險太高。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 6.1.6 選擇去識別化方法	組織應依據法律規定、組織任務、營運要求、資料使用對象及目的、所持有包含個資之資料內容、型式及數量、處理位置、資料揭露對象、揭露方式、揭露範圍及處理成本及風險評鑑結果等因素，選擇適宜之去識別化方法。此等去識別化方法須經組織之高階管理階層核准，且以文件記錄。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.1.7 全程受監督、留下紀錄	資料去識別化過程應留下紀錄、全程受監督(例：全程錄影)，且其紀錄應無法竄改，並定期稽核及不定期抽查紀錄。		☐符合 ☐不符合 ☐部分符合 ☐不適用
要求事項 (6. 2)	組織之高階管理階層應監督及審查個資去識別化過程之治理的安排。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.2.1 更新個資去識別化知識	組織應管理，關於個資去識別化之任何新指引、法規、法律、裁判、行政解釋、可用技術或威脅之相關知識，並據以評估風險。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 6.2.2 交流個資去識別化知識	組織應與同行業或從事類似工作之其他組織，分享並交流關於個資去識別化之知識。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.2.3 定期進行隱私衝擊評鑑	組織應定期對個資去識別化過程進行隱私衝擊評鑑(PIA)，並應公布其 PIA 報告(之適宜內容)，顯示如何處理風險評鑑過程。PIA 應包含所採用去識別化技術之有效性，以及評估重新識別之風險，以制定風險緩解措施。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.2.4 決定可接受剩餘風險準則	組織應訂定決定已移除個資之資料的可接受剩餘風險之準則。並應由組織之高階管理階層決定已移除個資之資料的可接受剩餘風險。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.2.5 審查去識別化過程時機	組織之高階管理階層應依規劃之期間或發生重大變更時審查去識別化過程。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 6.2.6 依回饋分析審查去識別化過程	組織應依據對來自利害相關者之回饋的分析，持續且及時審查個資去識別化過程。審查時應使用〝重新識別測試〞技術，評鑑重新識別風險及降低風險之措施。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.2.7 獨立之系統化檢查	組織應對已移除個資之所有資料，進行獨立(非原個資去識別化工作人員)之系統化(自動或人工)檢查。確保其中未包含直接識別資訊，以及非必要保留之間接識別資訊。並確保必要保留之間接識別資訊皆已(經由匿名化、擬匿名化或其他方法)合理去除與個資當事人之連結。		☐符合 ☐不符合 ☐部分符合 ☐不適用
要求事項 6.3	**組織應訂定個資去識別化過程之標準作業程序，並依此進行個資去識別化工作。**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.3.1 最少處理資料	組織應訂定標準作業程序，敘明如何依據處理後之資料用途，對將去識別化之資料集，依隱私權原則進行前置處理，僅取出最少需處理之資料集、內容、欄位或其部分。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 6.3.2 依資料型式選擇去識別作法及工具	組織應依待移除個資之資料型式(例：書面文字資料、書面圖片、文字檔、資料庫、圖片檔等)，以及不同檔案格式(例：DOC、DOCX、ODF、PDF、PPT、PPTX、TIF、JPG、MPEG、DICOM等)，選擇適當去識別作法及工具。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.3.3 建立重新識別威脅模型	組織應針對不同資料集，建立對經去識別化資料之重新識別威脅模型，進行隱私衝擊評鑑(PIA)，並依資料用途、釋出對象及方式、資料敏感性，設定可接受之剩餘風險值。可接受之剩餘風險值，應依個別個資當事人、部分個資當事人及所有涉及之個資當事人，分別設定特定值或平均值。各項可接受之剩餘風險值應由高階管理階層核可。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.3.4 設定推論控制值	組織應依資料釋出對象及方式、資料敏感性，設定推論控制之個別群組檻值(例：*k*-匿名性之最小 *k* 值、揭露筆數占整體筆數之最小百分比，或是差動隱私法之加雜訊參數值)。不得揭露不符合之資料。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 6.3.5 取樣測試	若資料集較大，為測試去識別化之效果，可能需先取樣測試。組織應訂定標準取樣程序，先依據信心水準及誤差率決定樣本資料數量，再由來源資料集之中，依隨機方式選取樣本資料。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.3.6 個資去識別化步驟	組織應訂定類似如下之個資去識別化步驟，並依此進行去識別化工作。 步驟 1：由領域專家(即有相關經驗人員)群判定最小可接受使用之資料集，並判定資料集之中各項資料之隱私等級。首先依據去識別化資料之用途，判定最小可接受使用之資料內容、欄位、範圍及數量，並據以判定可能需進行去識別化之資料的最大數量。再判定各項資料屬性(或欄位)係屬直接識別資料、間接識別資料、敏感資料或普通資料等。 步驟 2：將直接識別資料遮蔽(或變換)。即移除直接識別資料或將其匿名化。 步驟 3：針對不同資料屬性(或欄位)之間接識別與敏感資料，選定對應之去識別化方法。 步驟 4:建立對去識別化後資料		☐符合 ☐不符合 ☐部分符合 ☐不適用

	之威脅模型。於此步驟中，分析可能使用額外資訊或其他間接識別資料對已去識別化資料進行重新識別攻擊之各種情境，判定各種〝可能威脅〞。 步驟 5:使用步驟 4 所建立之模型，確定重新識別攻擊之風險的檻值。於此步驟中，組織判定使用已去識別化資料之可接受風險，以及可能降低風險之各項控制措施。 步驟 6：由來源資料庫取得(樣本)資料集，進行去識別化測試。若資料量較大，應依控制措施(6.3.5)，由來源資料庫中選取樣本資料。 步驟 7:評估實際之重新識別攻擊風險。即計算實際被重新識別之風險。 步驟 8:比較實際之被重新識別的風險與原設定可接受風險檻值。即比較步驟 7 與步驟 5 之結果。若實際風險值過高，則需考慮使用新的參數或去識別化方式(重複步驟 3 至步驟 8)。 步驟 9:設定去識別化參數並套		

	用至所有需去識別資料。若實際風險值小於最小可接受風險，則套用此等去識別化參數，並對選定資料進行去識別化。 步驟 10：對解決方案進行診斷。測試已去識別資料，以確保其具有足夠效用，並確認於允許之參數範圍內，合理之重新識別攻擊成功之機率小於可接受值。 步驟 11：輸出已去識別資料至外部資料集。於此最後步驟中，輸出已去識別化資料，並將所使用之去識別化技術、參數、威脅模型、風險值及各項相關資料，記錄於書面報告中。		
要求事項 6.4	**組織應備妥對個資遭非預期揭露之災難復原計畫。**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.4.1 及時因應申述及查詢	組織應及時回應來自自認為個人資料遭揭露民眾(或客戶)之申述及查詢，並依已建立之程序採取因應措施。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 6.4.2 備妥因應程序	組織應備妥程序，因應釋出資料遭重新識別而揭露個人隱私之情況，包含：移除可能揭露個人隱私之資料，重新處理；停止或修改(採取更嚴格之)去識別化過程。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.4.3 告知及協助當事人	當釋出資料遭重新識別而揭露個人隱私時，組織應告知隱私遭揭露之個人，並協助其採取必要之糾正及彌補措施。		☐符合 ☐不符合 ☐部分符合 ☐不適用
要求事項 6.5	**組織應備妥程序，對已移除個資之揭露資料，依可接受風險，定期進行〝重新識別測試〞。**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.5.1 揭露資料經匿名化或經不可逆之擬匿名處理	組織應對釋出及用以進行分析之已去識別化資料，經匿名化或經不可逆之擬匿名處理。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 6.5.2 選取測試樣本	若資料量巨大，無法對所有已去識別化資料進行〝重新識別測試〞(指於計算能力或經費上不可行)，組織應訂定依據信心水準及誤差率決定樣本資料數，由已去識別化資料中依隨機取樣方式選取測試樣本資料之標準作業程序。若僅測試樣本資料，而非所有資料，將會增加風險，應將此增加之風險納入風險估算。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.5.3 重新識別測試	組織應對擬公開釋出之所有已去識別化資料(或取樣資料)進行〝重新識別測試〞，至少包含下列項目： －搜尋網頁，嘗試連結個資當事人。 －搜尋全國或地方新聞資料庫，嘗試連結個資當事人。 －搜尋政府單位或其他組織之開放資料，嘗試連結個資當事人。 －以社群網路嘗試連結個資當事人。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.5.4 定期重新識別測試	因公眾可用之資料數量，隨時增長，故組織應定期重新對公開釋出之已去識別化資料進行〝重新識別測試〞，以重新評鑑其風險。若發現其風險超過檻值，組織應立即移除可能揭露個人隱私之資料，重新處理。並停止或修改(採取更嚴格之)去識別化過程。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 6.5.5 審核及管制資料流向及使用	組織若將已去識別化之資料授權(或委任)特定對象使用，則應備妥標準作業程序，審核及管制資料流向及使用，規定其用途、使用人員資格、使用人數，以及相關軟體、硬體網路及環境管制之要求事項。		☐符合 ☐不符合 ☐部分符合 ☐不適用
要求事項 6. 6	**(委外處理個資去識別化之要求)** **委外處理個資去識別化工作時，組織應監督、監視及稽核委外處理活動。**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.6.1 資料攜出需核准	原始資料以不攜出組織場域為原則。含有個資之限制資料複本，應經組織之高階管理階層核准方可攜出場域外。資料複本攜出場域外需滿足最小資料原則。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.6.2 資料傳送加密及保全	含有個資之限制資料複本，實體由組織移轉至受委託單位去識別化場所之過程應以秘密分享方案加密及保全，且過程應全程記錄及錄影。雖不建議，但組織若採取網路傳輸，移轉此等資料至受委託單位時，應使用足夠安全之加密方式，並透過專線或足夠安全之虛擬私有網路(VPN)以秘密分享方案傳送此等資料。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 6.6.3 委外契約規定	組織應與受委託單位簽定完善之委外契約，敘明受委託單位之相關義務與責任，以及契約終止條件。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.6.4 禁止進行其他處理及利用	組織應監督受委託單位依委託組織契約之要求，對所交付資料進行去識別化工作，不得進行其他處理及利用。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.6.5 實地稽核及抽查	組織應監督受委託單位之去識別化工作，定期實地稽核及不定期無預警抽查。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.6.6 妥善且安全保存資料	若資料複本攜出組織場域，受委託單位須依委託組織之隱私權政策及隱私權原則，全程妥善且安全保護原始資料及所處理資料。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.6.7 歸還銷毀所有持有資料	受委託單位於完成去識別化工作後，應立即將產出資料及原資料之複本歸還組織，且須確保安全的銷毀所有持有之受委託處理原始資料與產出資料。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 6.6.8 定期及不定期重新評估委外工作風險	組織應定期及不定期(例：發生重大事件時)，重新評估此項委外工作之風險並控制之。		☐符合 ☐不符合 ☐部分符合 ☐不適用
<u>要求事項 6.7</u>	**(對組織資料分析之要求事項)** **組織若對含有個資之(巨量)資料進行分析工作，應妥善保護隱私及設計資料分析機制。**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.7.1 判定供資料分析合法使用之個資去識別化程度	組織應備妥程序，判定供各項資料分析合法使用之個資去識別化程度。而於進行各批資料分析前，對應之去識別化程度，須經高階管理階層核定。且於完成資料去識別化後，須經獨立檢核其妥善性後，方可用於資料分析。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 6.7.2 僅提供經核定去識別化程度之資料	僅提供經事先核定去識別化程度之去識別化資料，供獲授權人員進行資料分析。 －應於合法且仍保持其效用之條件下，提供已去識別化之最高聚合程度資料，並盡可能提供最少個資細節。 －應盡可能隱藏資料中之個資及資料間之相互關係。		
控制措施 6.7.3 指定資料分析團隊及負責人	組織應指定資料分析團隊及負責人。應經由人員訓練，使團隊成員熟悉資料分析技術、隱私保護觀念、所涉及風險及減輕此等風險之措施。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.7.4 於管制環境進行資料分析	組織應備妥標準作業程序及完善之管制措施，將已適度去識別化資料置於管制環境中，僅供經授權之特定人員進行資料分析工作。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.7.5 合法及誠信原則	對含有個資之資料的分析工作，應符合〝合法及誠信原則〞。合法指對此等資料之分析符合相關法律規定，且若需個資當事人同意，已取得其同意。誠信指已明確且充分告知個資當事人其相關權利(例：可自由選擇撤回同意)。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 6.7.6 最少資料使用原則	對含有個資之資料的分析工作應符合〝最少資料使用原則〞，意指： — 將所涉及之個資數量、隱私權利害相關者數目及個資揭露對象或可存取個資之人員數目最小化。 — 確保採用〝僅知〞原則，亦即於合法分析條件下，僅對執行分析所必要之人員賦予資料取用權限。 — 一旦資料分析之目的終止，除依法需保存資料，或是實務上需保存資料，應即時刪除相關資料。保存之資料應加密，安全保存。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.7.7 預先設定之合法目的	組織應嚴格依〝預先設定之合法目的〞進行資料分析工作。確保分析目的均遵從適用之法律，且經高階管理階層預先設定。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.7.8 透明公開原則	組織對含有個資之資料的分析工作應符合〝透明公開原則〞。 －告知個資當事人，關於組織對於分析含有個資之資料的分析工作之政策、程序及實務的清楚且易取得之資訊。 －告知中包括，分析中之資料、分析目的、產出資料可能之應用及揭露對象之型式。 －告知組織提供予個資當事人之選擇及方式，以合法限制或移除分析其資料。		☐符合 ☐不符合 ☐部分符合 ☐不適用

	一當資料分析程序發生重大變更時，告知個資當事人。		
控制措施 6.7.9 資訊安全原則	對含有個資之資料的分析工作應符合〝資訊安全原則〞。以適宜之控制措施保護含有個資之資料。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.7.10 可歸責性	組織應記錄所有資料分析過程，並實施內部控制與稽核，以達成〝可歸責性〞。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.7.11 分離分析	組織應以分離方式分析不同來源之含有個資的資料，且同一個資當事人之資料應盡可能於不同系統中分析，避免不當連結，識別出個資當事人。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.7.12 管控分析產出結果流向及存取對象	組織若將分析之產出資料授權(或委任)予特定對象使用，則應備妥標準審核及管理程序，管制產出資料之流向、用途及使用者。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.7.13 由設計即保護隱私	組織實作含有個資之資料的分析過程，應遵循〝由設計即保護隱私(privacy by design, PbD)〞原則。亦即隱私保護遵循宜於系統設計時期即納入考量，而非於後續階段方納入。並將系統預設為隱私保護(privacy by default)。		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 6.7.14 當事人表達拒絕之處理	組織使用資料分析之產出(或已獲當事人同意直接使用其個資)於行銷(或提供服務選項)時，應提供當事人表示拒絕行銷(或服務選項)之管道。於當事人表達拒絕接受行銷(或服務選項)時，應立即停止對其行銷(或服務選項)，並周知所屬人員，或採行防範所屬人員再次行銷(或服務選項)之措施。		☐符合 ☐不符合 ☐部分符合 ☐不適用

柒、重新識別個資之要求

項目	**控制措施**	**文件名稱、章節出處或紀錄名稱**	**自評結果**
<u>要求事項 7.1</u>	**經匿名(或擬匿名)處理後資料之接收者應僅能鑑別個資當事人之資料屬性，而無法識別出個資當事人。**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 7.1.1 僅可查證但無法識別當事人	經匿名(或擬匿名)處理後之資料，不得提供任何可用以識別出個資當事人之資料，但必要時可允許資料接收者查證經匿名(或擬匿名)處理後之資料(或其屬性)是否真實。		☐符合 ☐不符合 ☐部分符合 ☐不適用
<u>要求事項 7.2</u>	同一個資當事人之經匿名(或擬匿名)處理後之不同資料，不得提供具有聚合後能連結至該個資當事人之資訊。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 7.2.1 聚合後不含可連結當事人資料	資料接收者取得之經匿名(或擬匿名)處理資料，不得包含可據以連結個資當事人之間接識別資料。		☐符合 ☐不符合 ☐部分符合 ☐不適用
<u>要求事項 7.3</u>	**資料經可逆之擬匿名處理後，應可於適當時(例如：法定之稽核)，由個資控制者重新識別個資當事人。**		☐符合 ☐不符合 ☐部分符合 ☐不適用

控制措施 7.3.1 秘密分享管制擬匿名法	組織若需採之擬匿名法進行個資去識別化，應使用加密法及秘密分享機制管制重新識別所需資訊。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 7.3.2 備有重新識別個資合法程序	必要時，組織應備有重新識別個資之合法程序，規定啟動時機、所使用方法、所需資訊、授權及啟動重新識別之流程。並依此啟動重新識別程序。對不同對象揭露個資時，宜使用不同擬匿名化函數或相同函數不同參數。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 7.3.3 定期審查程序之有效性	組織應定期審查合法重新識別個資之程序的有效性。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 7.3.4 能重新識別當事人	為使個資控制者之後能重新識別個資當事人，將資料經可逆之擬匿名處理後產生之紀錄單及重新識別所需之必要資料，應提供足以重新識別個資當事人之必要資訊。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 7.3.5 妥善加密持續保存紀錄單	組織對將個資資料經可逆之擬匿名處理所產生之紀錄單及重新識別所需之必要資料，應妥善加密，持續保存。		☐符合 ☐不符合 ☐部分符合 ☐不適用

<u>要求事項 7.4</u>	**於合法且有必要情況下(例如：法定之稽核)，組織應提供能正確重新識別個資當事人之證據。**		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 7.4.1 提供正確履行重新識別個資當事人之程序的證據	為避免不誠實宣稱，組織應提供正確履行重新識別個資當事人之程序的證據。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 7.4.2 記錄重新識別過程	組織於合法且有必要情況下，重新識別個資當事人資料之過程應留下紀錄、全程受監督(例：全程錄影)，且其紀錄應無法竄改。		☐符合 ☐不符合 ☐部分符合 ☐不適用

組織代表簽章：

附件二 聯邦貿易委員會案例探討

一、 背景說明

2014 年，美國聯邦貿易委員會（Federal Trade Commission, FTC）對我國華碩電腦股份有限公司（ASUSTeK Computer, Inc.）之路由器（Router）與雲端服務提出控訴，FTC 認為華碩公司在美國銷售的路由器產品存在安全性漏洞，致使消費者機敏資訊外洩。2016 年，華碩公司與 FTC 達成法律訴訟和解，華碩公司須提出產品資訊安全改善計畫，而且在未來 20 年內，其路由器與相關硬體裝置都須接受每 2 年一次的獨立第三方稽核。

2017 年，FTC 指控我國宏碁股份有限公司之路由器與網路攝影機存在安全性漏洞，使有心人士得以監控消費者位置，且未能確保消費者內容安全，包括所使用的登入軟體，此案件目前仍在在訴訟階段。

二、 FTC 提出的資安風險

1. 預設帳號密碼

華碩路由器預設帳號與密碼為 admin，非常容易猜到，其次也沒有強制要求使用者更改預設帳號與密碼，因此只要連網，就等同開放存取。

2. 軟體設計缺陷

駭客可透過路由器的 Web 介面控制平臺（web-based control panel）之設計漏洞取得控制權，透過遠端連線變更安全設定；

3. AiCloud 雲端服務設計缺陷

AiCloud 是一種雲端儲存服務，使用者可以將 USB 隨身碟連接到路由器的 USB 介面，類似外接硬體裝置，透過 Web 介面與行動應用存取隨身碟的檔案，使用者也可以經由 URL 管理分享其中的檔案與取消檔案存取。AiCloud 與路由器的登入帳號與密碼相同，而 AiCloud 存在未經認證存取用戶檔案與路由器登入憑證的漏洞，駭客只需掌握一組特定的 IP 位址，便可以繞過 AiCloud 的安全授權機制。其次，瀏覽與資料傳輸並無加密機制，登入資訊皆為明碼傳輸，很容易遭受中間人攻擊。

4. AiDisk 雲端服務設計缺陷

AiDisk 也是一種雲端儲存服務，使用者能夠建立自己的 FTP 伺服器，以 FTP 的方式連接路由器上的 USB 隨身碟，分享其中的資料，該服務缺乏傳輸資料的加密機制；其次，連接隨身碟的使用者並未設定瀏覽權限，預設帳號密碼為”Family”其安全性相對薄弱，只要取得路由器 IP 位址，等同將 USB 隨

身碟的資料公開在網路上。

5. 即時修補

AiCloud 與 AiDisk 的漏洞早在 FTC 提出前，就有資安專家回報這樣的漏洞訊息，但華碩公司並未告知使用者，同時在完成修補產品漏洞後，也沒有建議使用者立即修補產品漏洞，導致在 2014 年 2 月 AiDisk 發生大規模的使用者資料外洩事件。

其次，路由器上的檢查更新功能無法找到最新的韌體，因為檔案伺服器並未維護最新的可用韌體清單，導致更新時無法取得最新的韌體版本。

三、 安全建議

在物聯網發展趨勢下，許多物件具備連網功能，更突顯出路由器安全的重要性，FTC 站在使用者權益的角度，使大家意識到網路設備連網的安全風險，包括網路攝影機、網路儲存設備（Network Attached Storage, NAS）、連網家電等各式各樣的網路設備。國際間已有許多網路設備相關的資安標準與規範，例如 ISO 27001、UL2900 系列、GSMA IoT Security Guideline 等標準與指引文件，本計畫基於這些標準與指引文件，就 FTC 提出的路由器資安議題，提出相關的安全建議，如下說明。

1. 系統安全

網路設備的作業系統、網路服務、更新功能與韌體功能設計應具備足夠的安全防護。作業系統、網路服務與網頁管理介面不得存在常見的弱點與漏洞，可參考 NIST 提供的國家弱點資料庫（National Vulnerability Database）[52]；韌體須具備更新機制，線上更新路徑須具備安全通道功能，若為離線手動更新，則須進行加密保護，更新檔案也要具備完整性檢查功能；敏感性資料須具備加密或限制存取機制。漏洞修補或軟/韌體更新應讓使用者即時掌握，因為只有在使用者下載、安裝後，修補程式才能發揮作用。

2. 通訊安全

敏感性資料之網路傳輸需確保機密性，可使用 FIPS 140-2 核可之加密演算法；網路埠不得存取設備之作業系統；無線網路傳輸安全機制預設採用 WPA2 或更高安全性的協定。

3. 身分認證與授權機制

身分認證機制不得因重送攻擊而通過認證；認證錯誤訊息不得顯露合法使用者名稱等個人資訊；設備預設密碼不得重複；首次登入設備需強制更改

[52] https://nvd.nist.gov/

預設帳號、密碼；使用者需區分不同存取權限，除管理員為最高權限外，一般使用者建議設為「有限」權限，此部分也涵蓋雲端服務使用者的權限設定，避免不必要的資料外洩風險；登入頻率與次數須有相對限制；在設備獲得授權期間，一旦有遠端連線閒置、逾時、結束之情形，應要求新的認證。

4. 隱私保護

只有經過授權的使用者能存取設備所儲存的隱私資料；隱私資料不得明文傳輸，可使用 FIPS 140-2 核可之加密演算法。

四、 未來相關的資安風險

FTC 提出了長期以來所忽視的網路設備資安問題，特別是處於物聯網趨勢下的各種連網設備與平臺，無線路由器提供對外連網的能力，安全性更是首重課題，相較之下，無線接取更容易比有線網路存在資安風險。

附件三 業者訪談稿

有線電視業者個人資料與去識別的隱私規劃　訪談調查

2017/10/03

一、訪談提要

國家通訊傳播委員會委由財團法人電信技術中心辦理「通傳事業去識別化技術與相關技術規範研究」計畫，期盼透過國際通訊傳播事業用戶個人資料保護規範與去識別化機制研究，配合國內個人資料去識別化標準推展現況，制訂通訊傳播事業個人資料去識別化技術規範草案：

1. 物聯網— OTT 個人資料去識別化技術規範草案
2. 多媒體內容傳輸平台 MOD 個人資料去識別化技術規範草案
3. 有線電視個人資料去識別化技術規範草案

二、訪談目的

瞭解業者對於個人資料管控程序與隱私保護實務做法，以及對個人資料去識別化的看法與建議。

三、初步技術規範制訂方向

1. 隱私權政策與程序
2. 去識別化原則要求
3. 重新識別要求

四、訪談議題

項次		問題
資料蒐集與儲存	1.	對於使用服務的個人，貴公司所蒐集個資有哪些？
	2.	貴公司提供服務時，儲存/歸檔何種資料？（如：收視頻道、收視時段、收視時間、帳單明細等）？
	3.	是否提供互動性服務？蒐集之個人資料有哪些？儲存/歸檔何種資料？例如MOD服務訂閱影集、購物服務之購買物品等。
	4.	請說明問題1、2、3的回覆資料的儲存時限，依據的標準為何？
	5.	若貴公司根據預先訂定的時限儲存資料，當該時限屆滿時，貴公司作何處理？這方面貴公司有什麼規定的程序？
用戶權利與資料利用	6.	貴公司是否就問題 1、2、3所列儲存的資料，徵求用戶的同意？以何種方式徵求用戶同意？如不徵求用戶同意，請說明儲存這些資料的法律依據。
	7.	貴公司是否根據問題1、2、3的答覆所指的資料歸納整理用戶概況？如果是，為何目的？對何種資料進行處理？是否徵求用戶的同意？
	8.	如果貴公司除提供有線電視服務外，還提供其它服務，是否與該等服務共享貴公司透過有線電視服務蒐集的資料？反之是否亦然？如果是這樣，請說明共享的資料。
	9.	貴公司如何就個人資料的蒐集、處理及儲存等事項知會用戶？是否就諸如個人概況、收視偏好的歸納整理及其它互動活動的等事項向用戶提供資訊？
	10.	貴公司是否給用戶以查閱權及更正權，並按其要求更正、刪除與封存個人資料？
去識	11.	貴公司是否對個資作去識別化處理？如果是，請說明具體做法(如使用何種技術？)。如何確保不可逆？已作去識別化的資料包含何種資訊？

項次		問題
別化與資料控制	12.	個人資料之存取權限？資料電子化過程時，員工是否有相關安全管控措施？
	13.	貴公司是否向第三方傳送資料？請說明與以下哪些類型的公司分享。 • 數據分析公司； • 廣告商； • 子公司； • 其它- 請說明。
	14.	貴公司在個人資料保存是否採取安全措施？採取哪些措施？
其它	15.	對於本計畫之相關建議

MOD業者個人資料與去識別的隱私規劃　訪談調查

2017/10/03

一、訪談提要

國家通訊傳播委員會委由財團法人電信技術中心辦理「通傳事業去識別化技術與相關技術規範研究」計畫，期盼透過國際通訊傳播事業用戶個人資料保護規範與去識別化機制研究，配合國內個人資料去識別化標準推展現況，制訂通訊傳播事業個人資料去識別化技術規範草案：

1. 物聯網— OTT 個人資料去識別化技術規範草案
2. 多媒體內容傳輸平台 MOD 個人資料去識別化技術規範草案
3. 有線電視個人資料去識別化技術規範草案

二、訪談目的

瞭解業者對於個人資料管控程序與隱私保護實務做法，以及對個人資料去識別化的看法與建議。

三、初步技術規範制訂方向

1. 隱私權政策與程序
2. 去識別化原則要求
3. 重新識別要求

四、訪談議題

項次		問題
資料蒐集與儲存	1.	對於使用服務的個人，貴公司所蒐集個資有哪些？
	2.	貴公司提供服務時，儲存/歸檔何種資料？（如：收視頻道、收視時段、收視時間、帳單明細等）？
	3.	是否提供互動性服務？蒐集之個人資料有哪些？儲存/歸檔何種資料？例如MOD服務訂閱影集、購物服務之購買物品等。
	4.	請說明問題1、2、3的回覆資料的儲存時限，依據的標準為何？
	5.	若貴公司根據預先訂定的時限儲存資料，當該時限屆滿時，貴公司作何處理？這方面貴公司有什麼規定的程序？
用戶權利與資料利用	6.	貴公司是否就問題 1、2、3所列儲存的資料，徵求用戶的同意？以何種方式徵求用戶同意？如不徵求用戶同意，請說明儲存這些資料的法律依據。
	7.	貴公司是否根據問題1、2、3的答覆所指的資料歸納整理用戶概況？如果是，為何目的？對何種資料進行處理？是否徵求用戶的同意？
	8.	如果貴公司除提供有線電視服務外，還提供其它服務，是否與該等服務共享貴公司透過有線電視服務蒐集的資料？反之是否亦然？如果是這樣，請說明共享的資料。
	9.	貴公司如何就個人資料的蒐集、處理及儲存等事項知會用戶？是否就諸如個人概況、收視偏好的歸納整理及其它互動活動的等事項向用戶提供資訊？
	10.	貴公司是否給用戶以查閱權及更正權，並按其要求更正、刪除與封存個人資料？
去識	11.	貴公司是否對個資作去識別化處理？如果是，請說明具體做法(如使用何種技術？)。如何確保不可逆？已作去識別化的資料包含何種資訊？

項次		問題
別化與資料控制	12.	個人資料之存取權限？資料電子化過程時，員工是否有相關安全管控措施？
	13.	貴公司是否向第三方傳送資料？請說明與以下哪些類型的公司分享。 • 數據分析公司； • 廣告商； • 子公司； • 其它- 請說明。
	14.	貴公司在個人資料保存是否採取安全措施？採取哪些措施？
其它	15.	對於本計畫之相關建議